

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月 1日

出 願 番 号

Application Number:

特願2002-225277

[ST.10/C]:

[JP2002-225277]

出 願 人

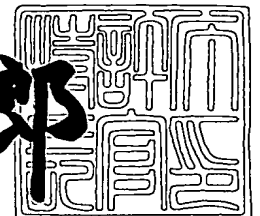
Applicant:

ソニー株式会社

2003年 5月27日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3039291

【書類名】 特許願

【整理番号】 0290442405

【提出日】 平成14年 8月 1日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 17/30

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号ソニー株式会社内

【氏名】 荻野 晃

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100082740

【弁理士】

【氏名又は名称】 田辺 恵基

【手数料の表示】

【予納台帳番号】 048253

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9709125

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ配信システム及びコンテンツ配信方法並びに端末装置

【特許請求の範囲】

【請求項 1】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記コンテンツに重畳する重畳手段と、

上記透かし情報が重畳されたコンテンツに所定の暗号をかける暗号化手段と、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する送信手段と

を具え、

上記端末装置では、

上記コンテンツを受信する受信手段と、

上記コンテンツに重畳されている上記透かし情報を所定の処理を行うようにして上記ユーザ識別情報及び上記格納定義フラグを抽出する抽出手段と、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記コンテンツにかけられている上記暗号を解除する暗号解除手段と、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、

上記判断手段の判断結果に応じて、上記透かし情報が重畳されているコンテンツを格納する格納手段と

を具えることを特徴とするコンテンツ配信システム。

【請求項 2】

上記ネットワーク上に設けられ、上記端末装置から発信されるコンテンツを監視しながら、当該コンテンツから上記ユーザ識別情報が検出された場合には、当

該端末装置に所定の通知又は警告を発信する監視サーバ

を具えることを特徴とする請求項 1 に記載のコンテンツ配信システム。

【請求項 3】

上記監視サーバは、

検出した上記ユーザ識別情報が上記端末装置に割り当てられた固有のユーザ識別情報と一致するか否かに応じて当該端末装置に上記通知又は上記警告を発信する

ことを特徴とする請求項 2 に記載のコンテンツ配信システム。

【請求項 4】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記コンテンツに重畳する第 1 のステップと、

上記透かし情報が重畳されたコンテンツに所定の暗号をかける第 2 のステップと、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する第 3 のステップと

を具え、

上記端末装置では、

上記コンテンツを受信する第 4 のステップと、

上記コンテンツに重畳されている上記透かし情報を所定の処理を行うようにして上記ユーザ識別情報及び上記格納定義フラグを抽出する第 5 のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記コンテンツにかけられている上記暗号を解除する第 6 のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除されたコンテンツを格納するか否かを判断する第 7 のステップと

上記判断結果に応じて、上記透かし情報が重畳されているコンテンツを格納する第 8 のステップと

を具えることを特徴とするコンテンツ配信方法。

【請求項 5】

上記ネットワーク上で上記端末装置から発信されるコンテンツを監視しながら、当該コンテンツから上記ユーザ識別情報が検出された場合には、当該端末装置に所定の通知又は警告を発信する第 9 のステップ

を具えることを特徴とする請求項 4 に記載のコンテンツ配信方法。

【請求項 6】

上記第 9 のステップでは、

検出した上記ユーザ識別情報が上記端末装置に割り当てられた固有のユーザ識別情報と一致するか否かに応じて当該端末装置に上記通知又は上記警告を発信する

ことを特徴とする請求項 5 に記載のコンテンツ配信方法。

【請求項 7】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを上記コンテンツに付加する第 1 のステップと、

上記ユーザ識別情報及び上記格納定義フラグが付加されたコンテンツに所定の暗号をかける第 2 のステップと、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する第 3 のステップと

を具え、

上記端末装置では、

上記コンテンツを受信する第 4 のステップと、

上記コンテンツに付加されている上記ユーザ識別情報及び上記格納定義フラグを抽出する第 5 のステップと、

上記格納定義フラグの状態に応じて上記コンテンツにかけられている上記暗号を解除する第 6 のステップと、

上記ユーザ識別情報の有効性に基づいて当該ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記コンテンツに重畳するか否かを判断する第 7 のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除された上記コンテンツを格納するか否かを判断する第 8 のステップと、

上記判断結果に応じて上記透かし情報が重畳されたコンテンツを格納する第 9 のステップと

を具えることを特徴とするコンテンツ配信方法。

【請求項 8】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを上記コンテンツに付加する第 1 のステップと、

上記ユーザ識別情報及び上記格納定義フラグが付加されたコンテンツに所定の暗号をかける第 2 のステップと、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する第 3 のステップと

を具え、

上記端末装置では、

上記コンテンツを受信して所定の格納手段に格納する第 4 のステップと、

上記格納手段から必要に応じて上記コンテンツを再生した場合、当該コンテンツに付加されている上記ユーザ識別情報及び上記格納定義フラグを抽出する第 5

のステップと、

上記格納定義フラグの状態に応じて上記コンテンツにかけられている上記暗号を解除する第 6 のステップと、

上記ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記暗号が解除された上記コンテンツに重畳する第 7 のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記透かし情報が重畳されたコンテンツを上記格納手段に格納するか否かを判断する第 8 のステップと、

上記判断結果に応じて上記透かし情報が重畳されたコンテンツを上記格納手段に格納する第 9 のステップと

を具えることを特徴とするコンテンツ配信方法。

【請求項 9】

コンテンツを管理する端末装置において、

上記コンテンツに、上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとが所定の拡散変調により変換された透かし情報として重畳されている場合、当該コンテンツに重畳されている上記透かし情報を所定の処理を行うようにして上記ユーザ識別情報及び上記格納定義フラグを抽出する抽出手段と、

上記コンテンツに暗号がかけられている場合、上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、当該コンテンツにかけられている上記暗号を解除する暗号解除手段と、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、

上記判断手段の判断結果に応じて、上記透かし情報が重畳されているコンテンツを格納する格納手段と

を具えることを特徴とする端末装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はコンテンツ配信システム及びコンテンツ配信方法並びに端末装置に関し、例えばインターネット等を用いたコンテンツ配信システムに適用して好適なものである。

【0002】

【従来の技術】

従来、この種のコンテンツ配信システムでは、配信側のサーバが、インターネット等のネットワークを介して接続された複数の個人端末のうちユーザからの要求等のあった個人端末に対して、文章、画像及び音声等の素材データを種々のシナリオで編集したデータ群（以下、これをコンテンツと呼ぶ）を配信するようになされている。

【0003】

その際、配信側のサーバは、該当するコンテンツを送信前に所定の暗号で暗号化する一方、ネットワークを介してコンテンツを受信したユーザ側の個人端末は、当該コンテンツにかけられた暗号を解除した場合のみ視聴することができるようになされた暗号化処理方式を採用するのが一般的である。

【0004】

【発明が解決しようとする課題】

ところが、かかる暗号化処理方式を採用したコンテンツ配信システムでは、ユーザによる最終的な視聴は暗号を解除した後でしか行い得ないため、個人端末におけるハードディスクや外部メモリ等に格納されているコンテンツが外部に取り出された場合には、当該コンテンツが不正に複製され、又はネットワーク上に流出された場合でも、そのようなリーケージパスを防ぐことは非常に困難であった。

【0005】

仮にこのような不正に複製され又はネットワーク上に流出されたコンテンツを発見した場合でも、当該コンテンツを不正に取得した者を特定することや、発見したコンテンツの同一性の確認を行うことが困難であることから、法的規制以外で不正流通の防止手段を講じる必要があった。

【 0 0 0 6 】

そしてこのようなデジタルコピーが容易に行われてしまうと、オリジナルのコンテンツと全く同じコピーができてしまうため、著作権保護を強化せざるを得ない状況となる。その結果、従来より一層、ユーザへの利用制限が厳しくなってしまう、正規にコンテンツを購入したユーザからは不満の声が上がる一方となるおそれがあった。

【 0 0 0 7 】

本発明は以上の点を考慮してなされたもので、正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム及びコンテンツ配信方法並びに端末装置を提案しようとするものである。

【 0 0 0 8 】

【課題を解決するための手段】

かかる課題を解決するため本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する重畳手段と、透かし情報が重畳されたコンテンツに所定の暗号をかける暗号化手段と、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する送信手段とを設け、端末装置では、コンテンツを受信する受信手段と、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けるようにした。

【 0 0 0 9 】

この結果このコンテンツ配信システムでは、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随する

こととなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【0010】

また本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する第1のステップと、透かし情報が重畳されたコンテンツに所定の暗号をかける第2のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第3のステップとを設け、端末装置では、コンテンツを受信する第4のステップと、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する第5のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する第6のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第7のステップと、判断結果に応じて、透かし情報が重畳されているコンテンツを格納する第8のステップとを設けるようにした。

【0011】

この結果このコンテンツ配信方法では、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【0012】

さらに本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第1のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第2のステップと、暗号が

けられたコンテンツをネットワークを介して端末装置に送信する第3のステップとを設け、端末装置では、コンテンツを受信する第4のステップと、コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第5のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第6のステップと、ユーザ識別情報の有効性に基づいて当該ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳するか否かを判断する第7のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第8のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納する第9のステップとを設けるようにした。

【0013】

この結果このコンテンツ配信方法では、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【0014】

さらに本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第1のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第2のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第3のステップとを設け、端末装置では、コンテンツを受信して所定の格納手段に格納する第4のステップと、格納手段から必要に応じてコンテンツを再生した場合、当該コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第5のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第6のステップと、ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を暗号が解除されたコンテンツに重畳する第7のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に

基づいて、透かし情報が重畳されたコンテンツを格納手段に格納するか否かを判断する第8のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納手段に格納する第9のステップとを設けるようにした。

【0015】

この結果このコンテンツ配信方法では、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【0016】

さらに本発明においては、コンテンツを管理する端末装置において、コンテンツに、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとが所定の拡散変調により変換された透かし情報として重畳されている場合、当該コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、コンテンツに暗号がかけられている場合、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、当該コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けるようにした。

【0017】

この結果この端末装置では、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【0018】

【発明の実施の形態】

以下図面について、本発明の一実施の形態を詳述する。

【0019】

(1) 第1の実施の形態

(1-1) 第1の実施の形態によるコンテンツ配信システムの全体構成

図1において、1は全体として本実施の形態によるコンテンツ配信システムを示し、ユーザが使用する複数の個人端末2 ($2_1 \sim 2_n$) と、サービス提供者側が配置した配信サーバ3及び監視サーバ4とがネットワーク5を介して接続されることにより構成されている。

【0020】

各個人端末2においては、一般家庭や会社内に設置された通常のパーソナルコンピュータであり、他の個人端末2や配信サーバ3とネットワーク5を介して通信することにより必要なデータを送受信したり、当該通信により得られた画面データに基づくWebページ画面等をディスプレイ表示することができるようになされている。

【0021】

また配信サーバ3は、サービス提供者側が提供する後述のような各種サービスに関する各種処理を行うWebサーバ及びデータベースサーバであり、ネットワーク5を介してアクセスしてきた個人端末2と通信して必要なコンテンツを送受信することができるようになされている。

【0022】

さらに監視サーバ4は、サービス提供者側が各個人端末2から発信されるコンテンツのうち著作権侵害に該当するコンテンツの有無をネットワーク上を常時巡回しながら監視し、著作権侵害に該当するコンテンツを検出した場合には、当該コンテンツを発信した個人端末に対して所定の警告をネットワークを介して通知することができるようになされている。

【0023】

(1-2) 配信サーバの具体的構成

ここで配信サーバ3の構成を図2に示す。この図2からも明らかなように、配信サーバ3は、配信サーバ3全体の制御を司るCPU (Central Processing Unit) 10と、各種ソフトウェアが格納されたROM (Read Only Memory) 11と、CPU10のワークメモリとしてのRAM (Random Access Memory) 12と、

各種データや種々のコンテンツが格納されたハードディスク装置（HDD）13と、CPU10がネットワーク5（図1）を介して外部と通信するためのインターフェースであるネットワークインターフェース部14と、フラッシュメモリ15と、ハードディスク装置13から音声情報でなるコンテンツが再生された場合に当該コンテンツに例えばATRAC3（Adaptive Transform Acoustic Coding 3）の音声圧縮処理を行う符号化部16と、圧縮符号化されたコンテンツに例えば公開鍵基盤（PKI：Public-key Infrastructure）等による暗号化処理を施す暗号化部17とを有し、これらがバスBUSを介して相互に接続されることにより構成されている。

【0024】

かかる構成に加えて、配信サーバ3は、フラッシュメモリ15から読み出された各種情報に所定の拡散変調（例えばスペクトラム拡散変調等）処理を施す拡散変調部19と、ハードディスク装置13から与えられたコンテンツに拡散変調部19から得られた後述する透かし情報を重畳させる重畳部18とを有し、当該透かし情報が重畳されたコンテンツを後段の符号化部16及び続く暗号化部17に供給するようになされている。

【0025】

まずCPU10は、ネットワーク5（図1）を介してアクセスしてきた個人端末2から与えられるデータやコマンドをネットワークインターフェース部14を介して取り込み、当該データやコマンドと、ROM11に格納されているソフトウェアとに基づいて各種処理を実行する。

【0026】

そしてCPU10は、この処理結果として、例えばハードディスク装置13から読み出した所定のコンテンツや、他のプログラム又はコマンドなどのデータを、必要に応じて暗号化等した後にネットワークインターフェース部14を介して対応する個人端末2に送出する。

【0027】

このようにして配信サーバ3においては、アクセスしてきた個人端末2に対してコンテンツやこの他の必要なデータを送受信し得るようになされている。なお

配信サーバ3のハードディスク装置13内にはそれぞれ複数のデータベース（図示せず）が格納されており、各種処理を実行するときに対応するデータベースから必要な情報を読み出し得るようになされている。

【0028】

（1-3）個人端末の具体的構成

図3に、各個人端末2における本体部2Hの内部構成を示す。各個人端末2の本体部2Hは、全体の制御を司るCPU20と、各種ソフトウェアが格納されたROM21と、CPU20のワークメモリとしてのRAM22、各種データが格納されたハードディスク装置23と、CPU20がネットワーク5（図1）を介して外部と通信するためのインターフェースであるネットワークインターフェース部24と、スピーカ25が接続された音声処理部26と、ディスプレイ27が接続された画像処理部28と、キーボード29及びマウス30が接続されたインターフェース部31と、ネットワークインターフェース部24を介して与えられたコンテンツにかけられた暗号を解除するデクリプト部32とを有し、これらがバスBUSを介して相互に接続されることにより構成されている。

【0029】

かかる構成に加えて、各個人端末2の本体部2Hは、各個人端末2の本体部2Hは、デクリプト部32において暗号が解除された後のコンテンツに重畳されている透かし情報を検出するID・フラグ検出部34と、当該ID・フラグ検出部32の検出結果に応じてコンテンツに所定の暗号をかける暗号化部35と、必要に応じて暗号解除処理を行うと共に圧縮処理されたコンテンツを元の状態に復元するデクリプト／復号化部36とを有する。

【0030】

まずCPU20は、ネットワーク5（図1）を介してアクセスしてきた配信サーバ3又は他の個人端末2から与えられるデータやコマンドをネットワークインターフェース部26を介して取り込み、当該データやコマンドと、ROM21に格納されているソフトウェアとに基づいて各種処理を実行する。

【0031】

そしてCPU20は、この処理結果として、例えばハードディスク装置23か

ら読み出した所定のコンテンツや他のプログラム又はコマンドなどのデータをネットワークインターフェース部 2 6 を介して配信サーバ 3 又は対応する他の個人端末 2 に送出する。

【 0 0 3 2 】

このようにして個人端末 2 においては、アクセスしてきた配信サーバ 3 又は他の個人端末に対して、コンテンツやこの他の必要なデータを送受信し得るようになされている。なお個人端末 2 のハードディスク装置 2 3 内にはそれぞれ複数のデータベース（図示せず）が格納されており、各種処理を実行するときに対応するデータベースから必要な情報を読み出し得るようになされている。

【 0 0 3 3 】

（ 1 - 4 ） 監視サーバの具体的構成

さらに監視サーバ 4 の構成を図 4 に示す。この監視サーバ 4 は、監視サーバ 4 全体の制御を司る CPU 4 0 と、各種ソフトウェアが格納された ROM 4 1 と、CPU 4 0 のワークメモリとしての RAM 4 2 と、各種データや種々のコンテンツが格納されたハードディスク装置 4 3 と、CPU 4 0 がネットワーク 5（図 1）を介して外部と通信するためのインターフェースであるネットワークインターフェース部 4 4 と、フラッシュメモリ 4 5 と、ネットワーク 5 上を巡回しながら不正なコンテンツを検出する不正コンテンツ検出部 4 6 とを有し、これらがバス BUS を介して相互に接続されることにより構成されている。

【 0 0 3 4 】

この監視サーバ 4 内のハードディスク装置 4 3 には、配信サーバ 3 に対して正規に登録した全ての個人端末 2 ごとにそれぞれ固有に割り当てられているユーザ識別情報 X_{ID} を保有するデータベース（図示せず）が格納されている。

【 0 0 3 5 】

不正コンテンツ検出部 4 6 は、例えば WinMX 及びグヌーテラ（Gnutella）等のファイル共有ソフトウェアを使用して、ネットワーク 5（図 1）上を巡回しながら各個人端末 2 から送信されるコンテンツを取得するようになされている。

【 0 0 3 6 】

そして不正コンテンツ検出部 4 6 は、取得したコンテンツに付加されているユ

ーザ識別情報 X_{ID} を検出して、コンテンツの発信元が正規登録したユーザの個人端末2に対応するユーザ識別情報 X_{ID} と一致するか否かを判断した後、一致する場合もしない場合にも当該コンテンツを発信した個人端末2に対して所定の通知又は警告をネットワーク5を介して通知するようになされている。

【0037】

(1-5) 配信サーバから個人端末へのコンテンツ配信

実際にこのコンテンツ配信システム1において、図2に示す配信サーバ3のCPU10は、個人端末2からアクセス要求があったとき、フラッシュメモリ15から当該個人端末2を所有するユーザに割り当てられたユーザ識別情報(ID) X_{ID} と、当該ユーザ識別情報 X_{ID} に付随して設けられた所定の判断用のフラグ(以下、これを格納定義フラグと呼ぶ) X_{FLG} とを読み出す。

【0038】

この格納定義フラグ X_{FLG} は、ユーザ側のデバイスである個人端末2内のハードディスク装置23にコンテンツを格納する際に、当該コンテンツを暗号化するか否かを判断するためのフラグであり、ユーザ識別情報 X_{ID} に付随して予めユーザによって立上り又は立下りが設定されている。

【0039】

続いて、配信サーバ3のCPU10は、フラッシュメモリ15から読み出したユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を拡散変調部19に送出する。拡散変調部19は、ユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} に所定の拡散変調処理を施すようにして透かし情報 X_{WM1} を生成する。

【0040】

この透かし情報 X_{WM1} は、いわゆる「電子透かし(Watermark)」と呼ばれる技術においてコンテンツの冗長部分に埋め込まれる著作権情報等であり、コンテンツの種類に応じてデータ内容が設定されるようになされている。

【0041】

例えばコンテンツが音声情報でなる場合、透かし情報 X_{WM1} は、一般に「強い音の直前直後の数10ミリ秒程度までにある微弱な音は強い音にかき消される」という人間の聴覚特性を利用することにより、当該コンテンツのうちの人間の聴

覚上重要でない部分に雑音として埋め込まれる。

【0042】

この後、配信サーバ3のCPU10は、拡散変調部19において拡散変調した透かし情報 X_{WM1} と、ハードディスク装置13から再生したユーザが所望するコンテンツD1とを重畳部18において重畳させるようにして合成情報データD2を生成する。

【0043】

具体的に合成情報データD2は、上述した電子透かしの技術に基づいて、コンテンツD1である音声情報を所定の標本化周波数（例えば44.1[kHz]）で標本化した後、下位ビットを探索して透かし情報 X_{WM1} を埋め込む手法や、フーリエ変換やウェーブレット変換を用いて音声情報であるコンテンツD1の波形分析を行った後に特定の周波数成分に透かし情報 X_{WM1} を埋め込む手法などにより生成される。

【0044】

続いて配信サーバ3のCPU10は、重畳部18から得られた合成情報データD2を符号化部16に送出して圧縮符号化させた後、続く暗号化部17において所定の暗号（以下、これを第1の暗号と呼ぶ）で暗号化させる。

【0045】

この後配信サーバ3のCPU10は、暗号化部17において暗号化した圧縮情報データ（以下、これを配信用コンテンツデータと呼ぶ）D3をネットワークインターフェイス部14を介してネットワーク5上に接続された対応する個人端末2に送信する。

【0046】

一方、このコンテンツ配信システム1において、図3に示す個人端末のCPU20は、図5に示すコンテンツ受信処理手順RT1をステップSP0から開始し、ネットワーク5（図1）を介して配信サーバ3から送信された配信用コンテンツデータD3をネットワークインターフェイス部24を介してデクリプト部32に送出する（ステップSP1）。

【0047】

このとき個人端末2のCPU20は、配信用コンテンツデータD3にユーザ識別情報 X_{ID} が付加されているか否かを判断し（ステップSP2）、当該ユーザ識別情報 X_{ID} が存在する場合のみ、デクリプト部32において上述の第1の暗号を解除するための暗号解除処理を継続する（ステップSP3）。

【0048】

一方、個人端末2のCPU20は、配信用コンテンツデータD3にユーザ識別情報 X_{ID} が付加されていないと判断した場合には、第1の暗号を解除しない旨を画像処理部28を介してディスプレイ27上に画面表示させるようにしてユーザに通知する（ステップSP4）。

【0049】

そして個人端末2のCPU20、デクリプト部32において暗号解除した配信用コンテンツデータ（以下、これを圧縮コンテンツデータと呼ぶ）D4を、ID・フラグ検出部34及び暗号化部35にそれぞれ送出する。

【0050】

ID・フラグ検出部34は、圧縮コンテンツデータD4に埋め込まれている透かし情報 X_{WM1} に逆拡散変調処理を施すことにより、当該透かし情報 X_{WM1} からユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出する。

【0051】

その際、個人端末2のCPU20は、RAM22から当該個人端末2に割り当てられているユーザ識別情報 X_{ID} を読み出して、これをID・フラグ検出部34において抽出されたユーザ識別情報 X_{ID} と照合して両者が一致するか否かを判断する（ステップSP5）。

【0052】

この判断結果が肯定的な場合には、個人端末2のCPU20は、ID・フラグ検出部34から抽出された格納定義フラグ X_{FLG} に基づいて、当該格納定義フラグ X_{FLG} の立上り又は立下りを検出し、当該検出結果に応じて、デクリプト部34から送出される圧縮コンテンツデータD4を暗号化するか否かを判断する（ステップSP6）。

【0053】

これに対してユーザ識別情報 X_{ID} の照合判断結果が否定的な場合には、個人端末2のCPU20は、コンテンツの受信が不可である旨を画像処理部28を介してディスプレイ27上に画面表示させるようにしてユーザに通知する（ステップSP7）。

【0054】

やがて暗号化部35は、個人端末2のCPU20から得られる格納定義フラグ X_{FLG} に応じた暗号化の有無結果に基づいて、暗号化する旨が得られた場合のみ、デクリプト部32から与えられた圧縮コンテンツデータD4に所定の暗号（以下、これを第2の暗号と呼ぶ。この暗号は第1の暗号と同一であってもよい。）をかける（ステップSP8）。

【0055】

続いて個人端末2のCPU20は、暗号化部35において必要に応じて第2の暗号がかけられた圧縮コンテンツデータD5をハードディスク装置23に格納する（ステップSP9）。

【0056】

この後、個人端末2のCPU20は、ユーザからマウス又はキーボード等による操作に基づく再生要求があったとき、ハードディスク装置23から対応する圧縮コンテンツデータD5を再生してデクリプト／復号化部36に送出する。

【0057】

デクリプト／復号化部36は、ハードディスク装置23から再生された圧縮コンテンツデータD5にかけられている第2の暗号を解除した後、圧縮処理された圧縮コンテンツデータD4を元の状態であるコンテンツD1に復元する（ステップSP10）。

【0058】

かくして個人端末2のCPU20は、デクリプト／復号化部36から得られた元のコンテンツD1を音声処理部26を介してスピーカ25から放音するようにしてユーザに提供する（ステップSP11）。

【0059】

（1-6）第1の実施の形態による動作及び効果

以上の構成において、このコンテンツ配信システム1では、配信サーバ3は、個人端末2からアクセス要求があったとき、当該個人端末2のユーザに関するユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を読み出して拡散変調することにより透かし情報 X_{WM1} を生成する。

【0060】

続いて配信サーバ3は、透かし情報 X_{WM1} を指定されたコンテンツD1に埋め込んだ後、第1の暗号をかけるようにして配信用コンテンツデータD3を生成し、これをネットワーク5を介してアクセス要求のあった個人端末2に送信する。

【0061】

かかる個人端末2では、配信サーバ3から送信される配信用コンテンツデータD3について、ユーザ識別情報 X_{ID} の存在を条件として第1の暗号を解除した後、圧縮コンテンツデータD4に埋め込まれている透かし情報 X_{WM1} からユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出する。

【0062】

そして個人端末2は、抽出したユーザ識別情報 X_{ID} が、配信サーバ3への登録時に当該個人端末2に割り当てられたユーザ識別情報 X_{ID} と一致し、かつ当該格納定義フラグ X_{FLG} が立上り状態である場合のみ、透かし情報 X_{WM1} が埋め込まれた圧縮コンテンツデータD4に第2の暗号をかけた後、ハードディスク装置23に格納する。

【0063】

このようにして個人端末2において、ネットワーク5を介して配信サーバ3からコンテンツを受信した際に、当該個人端末2内のハードディスク装置23には、コンテンツがユーザ識別情報 X_{ID} を透かし情報 X_{WM1} として埋め込まれた状態で格納されることにより、後にハードディスク装置23から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報 X_{ID} が付随することとなり、この結果、かかるコンテンツが不正に取得したものか否かを判断することができる。

【0064】

以上の構成によれば、コンテンツ配信システム 1 では、配信サーバ 3 において、ユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を透かし情報として埋め込んだコンテンツに第 1 の暗号をかけてアクセス要求のあった個人端末 2 にネットワークを介して送信する一方、当該個人端末 2 において、受信したコンテンツを、ユーザ識別情報 X_{ID} が存在した場合のみ第 1 の暗号を解除した後、当該ユーザ識別情報 X_{ID} が有効であり、かつ当該格納定義フラグ X_{FLG} が立上り状態である場合のみハードディスク装置 23 に格納するようにしたことにより、後にハードディスク装置 23 から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報 X_{ID} が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム 1 を実現することができる。

【 0 0 6 5 】

(2) 第 2 の実施の形態

(2-1) 第 2 の実施の形態におけるコンテンツ配信システムの全体構成

図 6 は、第 2 の実施の形態におけるコンテンツ配信システム 50 を示し、図 1 に示す第 1 の実施の形態におけるコンテンツ配信システム 1 とは、各個人端末 51 ($51_1 \sim 51_n$) 及び配信サーバ 52 の構成が異なることを除いて同様に構成されている。

【 0 0 6 6 】

(2-2) 第 2 実施の形態による配信サーバ及び個人端末の具体的構成

図 7 は第 2 の実施の形態による配信サーバ 52 を示し、図 2 に示す配信サーバ 3 とは、拡散変調部 19 (図 2) が取り除かれる以外は当該配信サーバ 3 と同様に構成されている。

【 0 0 6 7 】

この配信サーバ 52 では、CPU 10 がフラッシュメモリ 15 から読み出したユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を重畳部 18 において、ハードディスク装置 13 から再生されたコンテンツ D1 に重畳させた後、符号化部 16 及び続く暗号化部 17 に供給するようになされている。

【 0 0 6 8 】

また図 8 は第 2 の実施の形態による個人端末 5 1 を示し、図 3 に示す個人端末 2 とは、本体部 5 1 H 内において拡散変調部 5 5 及び重畳部 5 6 が加えられたことを除いて、当該個人端末 2 と同様に構成されている。

【 0 0 6 9 】

この個人端末 5 1 では、配信サーバ 5 2 (図 7) においてユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を「電子透かし」によるコンテンツへの埋め込み対象としなかった分、当該個人端末 5 1 において拡散変調部 5 5 がユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を拡散変調処理した後、重畳部 5 6 においてコンテンツの冗長部分に埋め込むようになされている。

【 0 0 7 0 】

(2 - 3) 配信サーバから個人端末へのコンテンツ配信

実際に図 7 に示す配信サーバ 5 2 の CPU 1 0 は、個人端末 5 1 (図 6) からアクセス要求があったとき、フラッシュメモリ 1 5 から当該個人端末 5 1 を所有するユーザに割り当てられたユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を読み出す。

【 0 0 7 1 】

続いて、配信サーバ 5 2 の CPU 1 0 は、フラッシュメモリ 1 5 から読み出したユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} と、ハードディスク装置 1 3 から再生したユーザが所望するコンテンツ D 1 とを重畳部 1 8 において重畳させるようにして合成情報データ D 1 0 を生成する。

【 0 0 7 2 】

具体的に合成情報データ D 1 0 は、上述した電子透かしの技術とは異なり、コンテンツ D 1 を構成する音声データ群のデータフォーマット内のヘッダ部分に書き込むことで生成されるようになされている。

【 0 0 7 3 】

続いて配信サーバ 5 2 の CPU 1 0 は、重畳部 1 8 から得られた合成情報データ D 1 0 を符号化部 1 6 に送出して圧縮符号化させた後、続く暗号化部 1 7 において第 1 の暗号で暗号化させる。

【 0 0 7 4 】

この後配信サーバ 5 2 の CPU 1 0 は、暗号化部 1 7 において暗号化した配信用コンテンツデータ D 1 1 をネットワークインターフェイス部 1 4 を介してネットワーク 5 上に接続された対応する個人端末 5 1 (図 6) に送信する。

【 0 0 7 5 】

一方、図 6 に示す個人端末 5 1 の CPU 2 0 は、図 9 に示すコンテンツ受信処理手順 R T 2 をステップ S P 2 0 から開始し、ネットワーク 5 (図 1) を介して配信サーバ 5 2 から送信された配信用コンテンツデータ D 1 1 をネットワークインターフェイス部 2 4 を介してデクリプト部 3 2 に送出する(ステップ S P 2 1)。

【 0 0 7 6 】

このとき個人端末 5 1 の CPU 2 0 は、配信用コンテンツデータ D 1 1 にユーザ識別情報 X_{ID} が付加されているか否かを判断し(ステップ S P 2 2)、当該ユーザ識別情報 X_{ID} が存在する場合のみ、デクリプト部 3 2 において上述の第 1 の暗号を解除するための暗号解除処理を行う(ステップ S P 2 3)。

【 0 0 7 7 】

一方、個人端末 5 1 の CPU 2 0 は、配信用コンテンツデータ D 1 1 にユーザ識別情報 X_{ID} が付加されていないと判断した場合には、第 1 の暗号を解除しない旨を画像処理部 2 8 を介してディスプレイ 2 7 上に画面表示させるようにしてユーザに通知する(ステップ S P 2 4)。

【 0 0 7 8 】

そして個人端末 5 1 の CPU 2 0 は、デクリプト部 3 2 において暗号解除された圧縮コンテンツデータ D 1 2 を、ID・フラグ検出部 3 4 及び重畳部 3 5 にそれぞれ送出する。

【 0 0 7 9 】

ID・フラグ検出部 3 4 は、圧縮コンテンツデータ D 1 2 からユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出する。その際、個人端末 5 1 の CPU 2 0 は、RAM 2 2 から当該個人端末 5 1 に割り当てられているユーザ識別情報 X_{ID} を読み出して、これを ID・フラグ検出部 3 4 において抽出されたユーザ

識別情報 X_{ID} と照合して両者が一致するか否かを判断する（ステップ SP 2 5）。

【 0 0 8 0 】

この判断結果が肯定的な場合には、個人端末 5 1 の CPU 2 0 は、ID・フラグ検出部 3 4 において抽出したユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} のうち、ユーザ識別情報 X_{ID} を拡張変調部 5 5 に送出させる一方、格納定義フラグ X_{FLG} を暗号化部 3 5 に送出させる（ステップ SP 2 6）。

【 0 0 8 1 】

これに対してユーザ識別情報 X_{ID} の照合判断結果が否定的な場合には、個人端末 5 1 の CPU 2 0 は、コンテンツの受信が不可である旨を画像処理部 2 8 を介してディスプレイ 2 7 上に画面表示させるようにしてユーザに通知する（ステップ SP 2 7）。

【 0 0 8 2 】

拡散変調部 5 5 は、ID・フラグ検出部 3 4 から与えられたユーザ識別情報 X_{ID} に所定の拡散変調処理を施すようにして透かし情報 X_{WM2} を生成する。この後、個人端末 5 1 の CPU 2 0 は、拡散変調部 5 5 において拡散変調した透かし情報 X_{WM2} と、デクリプト部 3 2 から送出される圧縮コンテンツデータ D 1 2 とを重畳部 5 6 において重畳させるようにして合成圧縮コンテンツデータ D 1 3 を生成する（ステップ SP 2 6）。

【 0 0 8 3 】

続いて個人端末 5 1 の CPU 2 0 は、ID・フラグ検出部 3 4 から抽出された格納定義フラグ X_{FLG} に基づいて、当該格納定義フラグ X_{FLG} の立上り又は立下りを検出し、当該検出結果に応じて、重畳部 5 6 から送出される合成圧縮コンテンツデータ D 1 3 を暗号化するか否かを判断する（ステップ SP 2 8）。

【 0 0 8 4 】

やがて暗号化部 3 5 は、個人端末 5 1 の CPU 2 0 から得られる格納定義フラグ X_{FLG} に応じた暗号化の有無結果に基づいて、暗号化する旨が得られた場合のみ、重畳部 5 6 から送出される合成圧縮コンテンツデータ D 1 3 に第 2 の暗号をかける（ステップ SP 2 9）。

【 0 0 8 5 】

これに対して暗号化しない旨が得られた場合には、暗号化部 3 5 は、第 2 の暗号をかけることなく、重畳部 5 6 から送出される合成圧縮コンテンツデータ D 1 3 をそのままハードディスク装置 2 3 に格納する（ステップ S P 3 0）。

【 0 0 8 6 】

続いて個人端末 5 1 の CPU 2 0、暗号化部 3 5 において必要に応じて第 2 の暗号がかけられた合成圧縮コンテンツデータ D 1 4 をハードディスク装置 2 3 に格納する（ステップ S P 3 0）。

【 0 0 8 7 】

この後、個人端末 5 1 の CPU 2 0 は、ユーザからマウス 2 9 又はキーボード 3 0 等による操作に基づく再生要求があったとき、ハードディスク装置 2 3 から対応する合成圧縮コンテンツデータ D 1 4 を再生してデクリプト／復号化部 3 6 に送出する。

【 0 0 8 8 】

デクリプト／復号化部 3 6 は、ハードディスク装置 2 3 から再生された合成圧縮コンテンツデータ D 1 4 にかけている第 2 の暗号を解除した後、圧縮処理された合成圧縮コンテンツデータ D 1 3 を元の状態であるコンテンツ D 1 に復元する（ステップ S P 3 1）。

【 0 0 8 9 】

かくして個人端末 5 1 の CPU 2 0、デクリプト／復号化部 3 6 から得られた元のコンテンツ D 1 を音声処理部 2 6 を介してスピーカ 2 5 から放音するようにしてユーザに提供する（ステップ S P 3 2）。

【 0 0 9 0 】

（ 2 - 4 ） 第 2 の実施の形態による動作及び効果

以上の構成において、このコンテンツ配信システム 5 0 では、配信サーバ 5 2 は、個人端末 5 1 からアクセス要求があったとき、当該個人端末 5 1 のユーザに関するユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を読み出した後、指定されたコンテンツ D 1 に重畳させて第 1 の暗号をかけるようにして配信用コンテンツデータ D 1 1 を生成し、これをネットワーク 5 を介してアクセス要求のあつ

た個人端末51に送信する。

【0091】

かかる個人端末51では、配信サーバ52から送信される配信用コンテンツデータD11について、ユーザ識別情報 X_{ID} の存在を条件として第1の暗号を解除した後、圧縮コンテンツデータD12からユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出する。

【0092】

続いて個人端末51は、抽出したユーザ識別情報 X_{ID} が、RAM22に格納されている当該個人端末51に割り当てられたユーザ識別情報 X_{ID} と一致する場合のみ、当該ユーザ識別情報 X_{ID} を拡散変調することにより透かし情報 X_{WM2} を生成すると共に、格納定義フラグ X_{FLG} の立上り状態を判断する。

【0093】

そして個人端末51は、格納定義フラグ X_{FLG} が立上り状態である場合のみ、透かし情報 X_{WM2} を圧縮コンテンツデータD12に埋め込むようにして合成圧縮コンテンツデータD13を生成し、さらに当該合成圧縮コンテンツデータD13に第2の暗号をかけた後、ハードディスク装置23に格納する。

【0094】

このようにして個人端末51において、ネットワーク5を介して配信サーバ52からコンテンツを受信した際に、当該個人端末51内のハードディスク装置23には、ユーザ識別情報 X_{ID} の有効性及び格納定義フラグ X_{FLG} の立上り状態を条件として当該ユーザ識別情報 X_{ID} を透かし情報 X_{WM2} としてコンテンツに埋め込んだ状態で格納することにより、後にハードディスク装置23から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報 X_{ID} が付随することとなり、この結果、かかるコンテンツが不正に取得したものか否かを判断することができる。

【0095】

以上の構成によれば、コンテンツ配信システム50では、配信サーバ3において、ユーザ識別情報 X_{ID} を重畳したコンテンツに第1の暗号をかけてアクセス要求のあった個人端末2にネットワークを介して送信する一方、当該個人端末2

において、受信したコンテンツを、ユーザ識別情報 X_{ID} が存在した場合のみ第1の暗号を解除した後、当該ユーザ識別情報 X_{ID} が有効であり、かつ格納定義フラグ X_{FLG} が立上り状態である場合のみ当該ユーザ識別情報 X_{ID} を透かし情報 X_{WM2} としてコンテンツに埋め込んだ状態でハードディスク装置23に格納するようにしたことにより、後にハードディスク装置23から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報 X_{ID} が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム50を実現することができる。

【0096】

(3) 第3の実施の形態

(3-1) 第3の実施の形態によるコンテンツ配信システムの構成

第3の実施の形態におけるコンテンツ配信システム（図示せず）は、図6に示す第2の実施の形態におけるコンテンツ配信システム50とは、各個人端末60（ $60_1 \sim 60_n$ ）の構成が異なることを除いて同様に構成されている。

【0097】

ここで図10に第3の実施の形態による個人端末60を示し、図8に示す個人端末51とは、本体部60H内においてID・フラグ検出部34及び暗号化部35に代えて、フラグ検出部61及び書込み部62が設けられていることを除いて、当該個人端末51とほぼ同様に構成されている。

【0098】

この個人端末60では、上述した第2の実施の形態における個人端末51のようにコンテンツにユーザ識別情報 X_{ID} を埋め込ませた後にハードディスク装置に格納させるのではなく、先にハードディスク装置にコンテンツを格納しておき、その後当該ハードディスク装置から再生したコンテンツにユーザ識別情報 X_{ID} を埋め込ませるようになっている。

【0099】

(3-2) 配信サーバから個人端末へのコンテンツ配信

図 1 0 に示す個人端末 6 0 の CPU 2 0 は、図 1 1 に示すコンテンツ受信処理手順 R T 3 をステップ S P 4 0 から開始し、ネットワーク 5 (図 1) を介して配信サーバ 5 2 から送信された配信用コンテンツデータ D 1 1 をネットワークインターフェイス部 2 4 を介してハードディスク装置 2 3 に格納する (ステップ S P 4 1 及び S P 4 2)。

【 0 1 0 0 】

この後、個人端末 6 0 の CPU 2 0 は、ユーザからマウス 2 9 又はキーボード 3 0 等による操作に基づく再生要求があったとき、ハードディスク装置 2 3 から対応する配信用コンテンツデータ D 1 1 を再生してデクリプト部 3 2 に送出する (ステップ S P 4 3)。

【 0 1 0 1 】

このとき個人端末 6 0 の CPU 2 0 は、配信用コンテンツデータ D 1 1 にユーザ識別情報 X_{ID} が付加されているか否かを判断し (ステップ S P 4 4)、当該ユーザ識別情報 X_{ID} が存在する場合のみ、デクリプト部 3 2 において上述の第 1 の暗号を解除するための暗号解除処理を行う (ステップ S P 4 5)。

【 0 1 0 2 】

一方、個人端末 6 0 の CPU 2 0 は、配信用コンテンツデータ D 1 1 にユーザ識別情報 X_{ID} が付加されていないと判断した場合には、第 1 の暗号を解除しない旨を画像処理部 2 8 を介してディスプレイ 2 7 上に画面表示させるようにしてユーザに通知する (ステップ S P 4 6)。

【 0 1 0 3 】

続いてデクリプト部 3 2 は、第 1 の暗号を解除した後の圧縮処理された圧縮コンテンツデータ D 1 2 をフラグ検出部 6 1 及び重畳部 5 6 に送出する。フラグ検出部 6 1 は、圧縮コンテンツデータ D 1 2 から格納定義フラグ X_{FLG} を抽出して重畳部 5 6 に送出する。

【 0 1 0 4 】

個人端末 6 0 の CPU 2 0 は、RAM 2 2 から当該個人端末 6 0 に割り当てられているユーザ識別情報 X_{ID} を読み出して、拡散変調部 5 5 において拡散変調させた後、透かし情報 X_{WM3} として重畳部 5 6 に送出させる。

【0105】

個人端末60のCPU20は、拡散変調部55において拡散変調した透かし情報 X_{WM3} と、デクリプト部32から送出される圧縮コンテンツデータD12と、フラグ検出部61から送出される格納定義フラグ X_{FLG} とを重畳部56において重畳させるようにして合成圧縮コンテンツデータD15を生成する。

【0106】

具体的に合成情報データD15は、上述した電子透かしの技術を用いて透かし情報 X_{WM3} がコンテンツに埋め込まれると共に、格納定義フラグ X_{FLG} がコンテンツを構成する音声データ群のデータフォーマット内のヘッダ部分に書き込むことで生成されるようになされている。

【0107】

続いて個人端末60のCPU20は、重畳部56から得られたが合成情報データD15を書込み部62を介してハードディスク装置23に格納させる。その際、個人端末60のCPU20は、ハードディスク装置23において、既に格納されている元の配信用コンテンツデータD11を消去して、新たに合成情報データD15を書き直す。

【0108】

この後、個人端末60のCPU20は、ユーザからマウス29又はキーボード30等による操作に基づく再生要求があったとき、ハードディスク装置23から対応する合成情報データD15を再生してデクリプト／復号化部36に送出する。

【0109】

デクリプト／復号化部36は、ハードディスク装置23から再生された圧縮処理されている合成情報データD15を元の状態であるコンテンツD1に復元する。

【0110】

かくして個人端末60のCPU20、デクリプト／復号化部36から得られた元のコンテンツD1を音声処理部26を介してスピーカ25から放音するようにしてユーザに提供する。

【 0 1 1 1 】

(3 - 3) 第 3 の実施の形態による動作及び効果

以上の構成において、このコンテンツ配信システムでは、配信サーバ 5 2 は、個人端末 6 0 からアクセス要求があったとき、当該個人端末 6 0 のユーザに関するユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を読み出した後、指定されたコンテンツ D 1 に重畳させて第 1 の暗号をかけるようにして配信用コンテンツデータ D 1 1 を生成し、これをネットワーク 5 を介してアクセス要求のあった個人端末 6 0 に送信する。

【 0 1 1 2 】

かかる個人端末 6 0 では、配信サーバ 5 2 から送信される配信用コンテンツデータ D 1 1 を一旦ハードディスク装置 2 3 に格納しておき、必要に応じて当該ハードディスク装置 2 3 から配信用コンテンツデータ D 1 1 を再生した後、ユーザ識別情報 X_{ID} の存在を条件として第 1 の暗号を解除する。

【 0 1 1 3 】

続いて個人端末 6 0 は、第 1 の暗号が解除された圧縮コンテンツデータ D 1 2 から格納定義フラグ X_{FLG} を抽出した後、RAM 2 2 に格納されている当該個人端末 5 1 に割り当てられたユーザ識別情報 X_{ID} を拡散変調することにより透かし情報 X_{WM3} を生成する。

【 0 1 1 4 】

そして個人端末 6 0 は、透かし情報 X_{WM3} と圧縮コンテンツデータ D 1 2 と格納定義フラグ X_{FLG} とを重畳させて合成圧縮コンテンツデータ D 1 5 を生成した後、これをハードディスク装置 2 3 に格納する。

【 0 1 1 5 】

このようにして個人端末 6 0 において、ネットワーク 5 を介して配信サーバ 5 2 からコンテンツを受信した際に、当該個人端末 6 0 内のハードディスク装置 2 3 には、一旦当該コンテンツを格納した後、必要に応じて再生した際に、ユーザ識別情報 X_{ID} を透かし情報 X_{WM3} としてコンテンツに埋め込んだ状態で再度格納することにより、後にハードディスク装置 2 3 から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報 X_{ID} が付随することとなり、この

結果、かかるコンテンツが不正に取得したものの可否かを判断することができる。

【0116】

以上の構成によれば、コンテンツ配信システム1では、配信サーバ3において、ユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を重畳したコンテンツに第1の暗号をかけてアクセス要求のあった個人端末2にネットワークを介して送信する一方、当該個人端末2において、受信したコンテンツを一旦当該コンテンツを格納した後、必要に応じて再生した際に、ユーザ識別情報 X_{ID} が存在した場合のみ第1の暗号を解除した後、ユーザ識別情報 X_{ID} を透かし情報 X_{WM3} としてコンテンツに埋め込んだ状態で再度格納することにより、後にハードディスク装置23から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報 X_{ID} が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システムを実現することができる。

【0117】

(4) 第1～第3の実施の形態における監視サーバによる警告

(4-1) 異なるユーザに基づくコンテンツ監視処理

上述した第1～第3の実施の形態において、図4に示す監視サーバ4は、ネットワーク5上を巡回しながら各個人端末2から送信されるコンテンツを取得し、当該コンテンツの発信元が正規登録したユーザの個人端末2であるか否かを検出して、当該検出結果に応じた通知又は警告をコンテンツを発信した個人端末に送信する。

【0118】

実際に監視サーバ4のCPU40は、図12に示すコンテンツ監視処理手順RT4をステップSP60から開始し、続くステップSP61に進んで、ネットワーク5を介して各個人端末からそれぞれコンテンツ（コンテンツ配信データ）を取得する。

【0119】

監視サーバ4のCPU40は、ステップSP62において、取得したコンテ

ツ（コンテンツ配信データ）にユーザ識別情報 X_{ID} が付加されているか否かを判断し、当該ユーザ識別情報 X_{ID} が存在する場合のみ、ステップSP63に進んで、ネットワーク5を介して配信サーバから当該コンテンツの発信元である個人端末に割り当てられているユーザ識別情報 X_{ID} を取得する。

【0120】

監視サーバ4のCPU40は、ステップSP64に進んで、不正コンテンツ検出部46において、コンテンツ（コンテンツ配信データ）から得られたユーザ識別情報 X_{ID} と、配信サーバから取得したユーザ識別情報 X_{ID} とを照合して両者が一致するか否かを判断する。

【0121】

このステップSP64における判断結果が肯定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末であることを表しており、このとき監視サーバ4のCPU40は、ステップSP65に進んで、不正コンテンツ検出部46において、例えば「あなたが所有するコンテンツがネットワーク上に流出していますよ。」のような所定の通知が記述された通知データをネットワークを介して正規登録しているユーザがもつ個人端末に送信する。

【0122】

この後、監視サーバ4のCPU40は再度ステップSP61に戻って、上述と同様にネットワーク5上を巡回しながら不正なコンテンツの流出を検出し続ける。

【0123】

これに対してステップSP64における判断結果が否定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末と異なることを表しており、このとき監視サーバ4のCPU40は、ステップSP66に進んで、不正コンテンツ検出部46において、例えば「あなたは他人のコンテンツを不正にネットワーク5上に流出させており、かかる行為は著作権法に違反しているため罰せられますよ。」のような所定の警告が記述された警告データをネットワークを介して当該コンテンツを発信した個人端

末に送信する。

【0124】

この後、監視サーバ4のCPU40は再度ステップSP61に戻って、上述と同様にネットワーク5上を巡回しながら不正なコンテンツの流出を検出し続ける。

【0125】

このように監視サーバ4では、各個人端末2から発信されるコンテンツをネットワーク5上を常時巡回しながら監視し、ネットワーク5上に流出したコンテンツを検出した場合には、当該コンテンツを発信した個人端末2に対して所定の通知又は警告を発信することにより、当該コンテンツの発信者にその旨を認識させることができ、かくしてネットワーク5上に流出したコンテンツの著作権が侵害されるのを未然に防止することができる。

【0126】

(4-2) ファイル共有に基づくコンテンツ監視処理

上述した第1～第3の実施の形態において、図4に示す監視サーバ4は、ネットワーク5上を巡回しながら各個人端末から送信されるコンテンツを取得し、共有ファイルを提供するユーザの個人端末が当該コンテンツの発信元が正規登録したユーザの個人端末であるか否かを検出して、当該検出結果に応じた通知又は警告をコンテンツを発信した個人端末に送信する。

【0127】

実際に監視サーバ4のCPU40は、図13に示すコンテンツ監視処理手順RT5をステップSP70から開始し、続くステップSP71に進んで、ファイル共有ソフトウェアを使用して、ネットワーク5を介して各個人端末からそれぞれコンテンツ（コンテンツ配信データ）を取得する。

【0128】

監視サーバ4のCPU40は、ステップSP72において、取得したコンテンツ（コンテンツ配信データ）にユーザ識別情報X_{ID}が付加されているか否かを判断し、当該ユーザ識別情報X_{ID}が存在する場合のみ、ステップSP73に進んで、取得したコンテンツから共有ファイルに基づくIPアドレス、MACアド

レス及び日時等の関連情報を取得した後、ステップ S P 7 4 に進んで、当該関連情報をネットワーク 5 を介して配信サーバに送信する。

【 0 1 2 9 】

やがて監視サーバ 4 の C P U 4 0 は、ステップ S P 7 5 に進んで、ネットワーク 5 を介して配信サーバから当該コンテンツの発信元である個人端末に割り当てられているユーザ識別情報 X _{I D} を取得した後、ステップ S P 7 6 に進んで、不正コンテンツ検出部 4 6 において、当該取得したユーザ識別情報 X _{I D} と、コンテンツ（コンテンツ配信データ）から得られたユーザ識別情報 X _{I D} とを照合して両者が一致するか否かを判断する。

【 0 1 3 0 】

このステップ S P 7 6 における判断結果が肯定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末であることを表しており、このとき監視サーバ 4 の C P U 4 0 は、ステップ S P 7 7 に進んで、不正コンテンツ検出部 4 6 において、例えば「あなたが所有するコンテンツがネットワーク上に流出していますよ。」のような所定の通知が記述された通知データをネットワーク 5 を介して正規登録しているユーザがもつ個人端末に送信する。

【 0 1 3 1 】

この後、監視サーバ 4 の C P U 4 0 は再度ステップ S P 7 1 に戻って、上述と同様にネットワーク 5 上を巡回しながら不正なコンテンツの流出を検出し続ける。

【 0 1 3 2 】

これに対してステップ S P 7 6 における判断結果が否定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末と異なることを表しており、このとき監視サーバ 4 の C P U 4 0 は、ステップ S P 7 8 に進んで、不正コンテンツ検出部 4 6 において、例えば「あなたは他人のコンテンツを不正にネットワーク上に流出させており、かかる行為は著作権法に違反しているため罰せられますよ。」のような所定の警告が記述された警告データをネットワーク 5 を介して当該コンテンツを発信した個人端

末に送信する。

【 0 1 3 3 】

この後、監視サーバ4のCPU40は再度ステップSP71に戻って、上述と同様にネットワーク5上を巡回しながら不正なコンテンツの流出を検出し続ける。

【 0 1 3 4 】

このように監視サーバ4では、各個人端末2から発信されるコンテンツをネットワーク5上を常時巡回しながら監視し、ネットワーク5上に流出したコンテンツを検出した場合には、当該コンテンツを発信した共有ファイルを提供するユーザの個人端末2に対して所定の通知又は警告を発信することにより、当該コンテンツの発信者にその旨を認識させることができ、かくしてネットワーク5上に流出したコンテンツの著作権が侵害されるのを未然に防止することができる。

【 0 1 3 5 】

(5) 他の実施の形態

なお上述のように第1～第3の実施の形態においては、本発明を図1及び図6のように構成された各個人端末（端末装置）2、51、60及び配信サーバ3、52からなるコンテンツ配信システム1、50に適用するようにした場合について述べたが、本発明はこれに限らず、これ以外の形態のこの他種々の構成のコンテンツ配信システムに広く適用することができる。

【 0 1 3 6 】

さらに上述のように第1～第3の実施の形態においては、各個人端末（端末装置）2、51、60及び配信サーバ3、52間では、インターネット等のネットワーク5を介して相互に接続するようにした場合について述べたが、本発明はこれに限らず、これ以外にも一般公衆回線やLAN（Local Area Network）等の有線通信回線網のみならず無線通信回線網からなるネットワークに広く適用することができる。

【 0 1 3 7 】

また各個人端末（端末装置）2、51、60及び配信サーバ3、52間では、ネットワークを介することなく、配信サーバ3、52から各個人端末（端末装置

） 2、51、60 にコンテンツをいわゆるパッケージメディア（既製品のメディア）として送付するようにしても良い。この場合、ユーザは、予め個人端末の購入時、メディアの購入時又はコンテンツの使用前までに、固有のユーザ識別情報を本人認証を前提として配信サーバに登録しておき、当該配信サーバで管理するようにしておく必要がある。その際、配信サーバは、必要に応じてユーザ識別情報を暗号化しておき、使用時にユーザ認証を行わせるようにしても良い。

【 0 1 3 8 】

さらに上述の第 1 ～ 第 3 の実施の形態においては、配信サーバ 3、52 においてコンテンツに暗号（第 1 の暗号）をかけて送信する一方、個人端末（端末装置） 2、51、60 においてユーザ識別情報 X_{ID} の存在を条件として当該コンテンツから暗号（第 1 の暗号）を解除した後、当該ユーザ識別情報 X_{ID} が有効であり、かつ格納定義フラグ X_{FLG} が立上り状態である場合のみ当該コンテンツに第 2 の暗号をかけてハードディスク装置（格納手段） 23 に格納するようにした場合について述べたが、本発明はこれに限らず、このような個人端末（端末装置） 2、51、60 側で再暗号化することなく、個人端末（端末装置） 2、51、60 において、配信サーバ 3、52 から受信したコンテンツにかけられている暗号（第 1 の暗号）をユーザ識別情報 X_{ID} 及び又は格納定義フラグ X_{FLG} に基づいて暗号解除して格納するか否かを判断した後でハードディスク装置（格納手段） 23 に格納するようにしても良い。

【 0 1 3 9 】

さらに上述の第 1 ～ 第 3 の実施の形態においては、配信サーバ 3、52 でコンテンツに付加される格納定義フラグ X_{FLG} を、個人端末（端末装置） 2、51、60 において暗号の解除又は非解除の判断基準とするようにした場合について述べたが、本発明はこれに限らず、個人端末（端末装置） 2、51、60 を所有するユーザの選択に応じて暗号の解除又は非解除を決定するようにしても良いし、併用するようにしても構わない。この場合、暗号の解除又は非解除は、ユーザごと及び又はコンテンツごとに設定するようにしても良い。

【 0 1 4 0 】

さらに上述の第 1 ～ 第 3 の実施の形態においては、配信サーバ 3、52 又は個

人端末（端末装置）2、51、60でユーザ識別情報 X_{ID} を、例えばスペクトラム拡散変調等の拡散変調処理により電子透かし（Watermark）と呼ばれる透かし情報に変換するようにした場合について述べたが、本発明はこれに限らず、要はコンテンツに著作権情報として埋め込むことができれば、この他例えばステガノグラフィ（Steganography）等の暗号技術を適用するようにしても良い。

【0141】

さらに上述の第1～第3の実施の形態においては、配信サーバ3、52に登録されるユーザ識別情報 X_{ID} として、個人端末（端末装置）2、51、60を所有するユーザに割り当てられたユーザIDを適用するようにした場合について述べたが、本発明はこれに限らず、IPv6（internet protocol version 6）やIPv4（internet protocol version 4）等のインターネット・プロトコルのバージョンで表現されるIPアドレス、パスワード、プロバイダ名、電子メールアドレス、さらには公的機関又はそれに順ずる機関が発行するIDや証明書番号、日時、国名、電話番号、端末装置名及び製造時のシリアル番号や機器ID等を広く適用するようにしても良い。

【0142】

さらに上述の第1～第3の実施の形態においては、ネットワーク5上に設けられ、個人端末（端末装置）2、51、60から発信されるコンテンツを監視しながら、当該コンテンツからユーザ識別情報 X_{ID} が検出された場合には、当該ユーザ識別情報 X_{ID} が個人端末（端末装置）2、51、60に割り当てられた固有のユーザ識別情報 X_{ID} と一致するか否かに応じて当該個人端末（端末装置）2、51、60に所定の通知又は警告を発信する監視サーバ4を構築するようにした場合について述べたが、本発明はこれに限らず、要はネットワーク上にコンテンツを流出したユーザに通知又は警告を与えることができれば、この他種々の構成からなる監視サーバに広く適用することができる。

【0143】

さらに上述のように第1の実施の形態においては、配信サーバ3及び端末装置2がネットワーク5を介して接続されたコンテンツ配信システム1において、配信サーバ3では、端末装置2に割り当てられた固有のユーザ識別情報 X_{ID} と、

端末装置 2 側で予め状態が設定された格納定義フラグ X_{FLG} とを所定の拡散変調を行うようにして透かし情報 X_{WM1} に変換した後、当該透かし情報 X_{WM1} をコンテンツに重畳する重畳部 1 8、拡散変調部 1 9（重畳手段）と、透かし情報 X_{WM1} が重畳されたコンテンツに所定の暗号をかける暗号化部（暗号化手段）1 7 と、暗号がかけられたコンテンツをネットワーク 5 を介して端末装置 2 に送信する送信手段 1 4 とを設け、端末装置 2 では、コンテンツを受信するネットワークインターフェイス（受信手段）2 4 と、コンテンツに重畳されている透かし情報 X_{WM1} を所定の処理を行うようにしてユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出する ID・フラグ検出部（抽出手段）3 4 と、ユーザ識別情報 X_{ID} の有効性及び又は格納定義フラグ X_{FLG} の状態に基づいて、コンテンツにかけられている暗号を解除するデクリプト部（暗号解除手段）3 2 と、ユーザ識別情報 X_{ID} の有効性及び又は格納定義フラグ X_{FLG} の状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する CPU（判断手段）2 0 と、判断手段 2 0 の判断結果に応じて、透かし情報 X_{WM1} が重畳されているコンテンツを格納するハードディスク装置（格納手段）2 3 とを有するようにしてコンテンツ配信システム 1 を構築するようにした場合について述べたが、本発明はこれに限らず、これ以外にも配信サーバ 3 が個人端末（端末装置）2 側で設定したユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を透かし情報 X_{WM1} としてコンテンツと共に当該個人端末（端末装置）2 に送信することができれば、この他種々の配信サーバ及び端末装置に広く適用することができる。

【0 1 4 4】

またユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} は、拡散変調による透かし情報とするに限らず、そのままフラグ情報として、コンテンツに付加されるようにしてもよい。個人端末（端末装置）側においても、暗号化コンテンツの場合は、セキュリティーが確保されているので、透かし情報を検出せずに、このフラグ情報だけを読むようにしてもよい。

【0 1 4 5】

さらに上述のように第 2 の実施の形態においては、配信サーバ 5 2 では、個人端末（端末装置）5 1 に割り当てられた固有のユーザ識別情報 X_{ID} 及び当該端

末装置側で予め状態が設定された格納定義フラグ X_{FLG} をコンテンツに付加する一方、個人端末（端末装置）51では、受信したコンテンツに付加されているユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出して、当該格納定義フラグ X_{FLG} の状態に応じてコンテンツにかけられている暗号を解除し、ユーザ識別情報 X_{ID} の有効性に基づいて当該ユーザ識別情報 X_{ID} を所定の拡散変調を行うようにして透かし情報 X_{WM2} に変換した後、当該透かし情報 X_{WM2} をコンテンツに重畳するか否かを判断する。そしてユーザ識別情報 X_{ID} の有効性及び又は格納定義フラグ X_{FLG} の状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断して、判断結果に応じて透かし情報 X_{WM2} が重畳されたコンテンツを格納するようにした場合について述べたが、本発明はこれに限らず、要は個人端末（端末装置）51においてユーザ識別情報 X_{ID} を透かし情報 X_{WM2} としてコンテンツにユーザ識別情報 X_{ID} を重畳することができれば、この他種々の構成の配信サーバ及び端末装置に広く適用するようにしても良い。

【 0 1 4 6 】

さらに上述のように第3の実施の形態においては、配信サーバ52では、個人端末（端末装置）60に割り当てられた固有のユーザ識別情報 X_{ID} 及び当該端末装置側で予め状態が設定された格納定義フラグ X_{FLG} をコンテンツに付加する一方、個人端末（端末装置）60では、コンテンツを受信してハードディスク装置（格納手段）23に格納しておき、当該ハードディスク装置（格納手段）23から必要に応じてコンテンツを再生した場合、当該コンテンツに付加されているユーザ識別情報 X_{ID} 及び格納定義フラグ X_{FLG} を抽出して、当該格納定義フラグ X_{FLG} の状態に応じてコンテンツにかけられている暗号を解除し、ユーザ識別情報 X_{ID} を所定の拡散変調を行うようにして透かし情報 X_{WM3} に変換した後、当該透かし情報 X_{WM3} を暗号が解除されたコンテンツに重畳する。そしてユーザ識別情報 X_{ID} の有効性及び又は格納定義フラグ X_{FLG} の状態に基づいて、透かし情報 X_{WM3} が重畳されたコンテンツをハードディスク装置（格納手段）23に格納するか否かを判断して、判断結果に応じて透かし情報 X_{WM3} が重畳されたコンテンツをハードディスク装置（格納手段）23に格納するよ

うにした場合について述べたが、本発明はこれに限らず、要は個人端末（端末装置）60においてユーザ識別情報 X_{ID} を透かし情報 X_{WM3} としてコンテンツにユーザ識別情報 X_{ID} を重畳することができれば、コンテンツをハードディスク装置（格納手段）23に格納する前後にかかわらず、この他種々の構成の配信サーバ及び端末装置に広く適用するようにしても良い。

【0147】

【発明の効果】

上述のように本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する重畳手段と、透かし情報が重畳されたコンテンツに所定の暗号をかける暗号化手段と、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する送信手段とを設け、端末装置では、コンテンツを受信する受信手段と、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するかどうかを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システムを実現できる。

【0148】

また本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた

固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する第1のステップと、透かし情報が重畳されたコンテンツに所定の暗号をかける第2のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第3のステップとを設け、端末装置では、コンテンツを受信する第4のステップと、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する第5のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する第6のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第7のステップと、判断結果に応じて、透かし情報が重畳されているコンテンツを格納する第8のステップとを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信方法を実現できる。

【 0 1 4 9 】

さらに本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第1のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第2のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第3のステップとを設け、端末装置では、コンテンツを受信する第4のステップと、コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第5のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第6のステップと、ユーザ識別情報の有効性に基づいて当該ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテ

ンツに重畳するか否かを判断する第7のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第8のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納する第9のステップとを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信方法を実現できる。

【 0 1 5 0 】

さらに本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第1のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第2のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第3のステップとを設け、端末装置では、コンテンツを受信して所定の格納手段に格納する第4のステップと、格納手段から必要に応じてコンテンツを再生した場合、当該コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第5のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第6のステップと、ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を暗号が解除されたコンテンツに重畳する第7のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、透かし情報が重畳されたコンテンツを格納手段に格納するか否かを判断する第8のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納手段に格納する第9のステップとを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして

正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信方法を実現できる。

【 0 1 5 1 】

さらに本発明によれば、コンテンツを管理する端末装置において、コンテンツに、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとが所定の拡散変調により変換された透かし情報として重畳されている場合、当該コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、コンテンツに暗号がかけられている場合、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、当該コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けたことにより、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得る端末装置を実現できる。

【図面の簡単な説明】

【図 1】

第 1 の実施の形態によるコンテンツ配信システムの構成を示す略線図である。

【図 2】

図 1 に示す配信サーバの内部構成を示すブロック図である。

【図 3】

図 1 に示す個人端末の内部構成を示すブロック図である。

【図 4】

図 1 に示す監視サーバの内部構成を示すブロック図である。

【図 5】

第 1 の実施の形態によるコンテンツ受信処理手順の説明に供するフローチャー

トである。

【図 6】

第 2 の実施の形態によるコンテンツ配信システムの構成を示す略線図である。

【図 7】

図 6 に示す配信サーバの内部構成を示すブロック図である。

【図 8】

図 6 に示す個人端末の内部構成を示すブロック図である。

【図 9】

第 2 の実施の形態によるコンテンツ受信処理手順の説明に供するフローチャートである。

【図 1 0】

第 3 の実施の形態による個人端末の構成を示すブロック図である。

【図 1 1】

第 3 の実施の形態によるコンテンツ受信処理手順の説明に供するフローチャートである。

【図 1 2】

第 1 ～第 3 の実施の形態による異なるユーザに基づくコンテンツ監視処理手順の説明に供するフローチャートである。

【図 1 3】

第 1 ～第 3 の実施の形態によるファイル共有に基づくコンテンツ監視処理手順の説明に供するフローチャートである。

【符号の説明】

1、5 0 ……コンテンツ配信システム、2、5 1 ……個人端末、3、5 2 ……配信サーバ、4 ……監視サーバ、5 ……ネットワーク、1 0、2 0、4 0 ……C P U、1 3、2 3、4 3 ……ハードディスク装置、1 8、5 6 ……重畳部、1 9、5 5 ……拡散変調部、3 4 ……I D・フラグ検出部、4 6 ……不正コンテンツ検出部 4 6、R T 1 ～R T 3 ……コンテンツ受信処理手順、R T 4、R T 5 ……コンテンツ監視処理手順。

【書類名】図面

【図1】

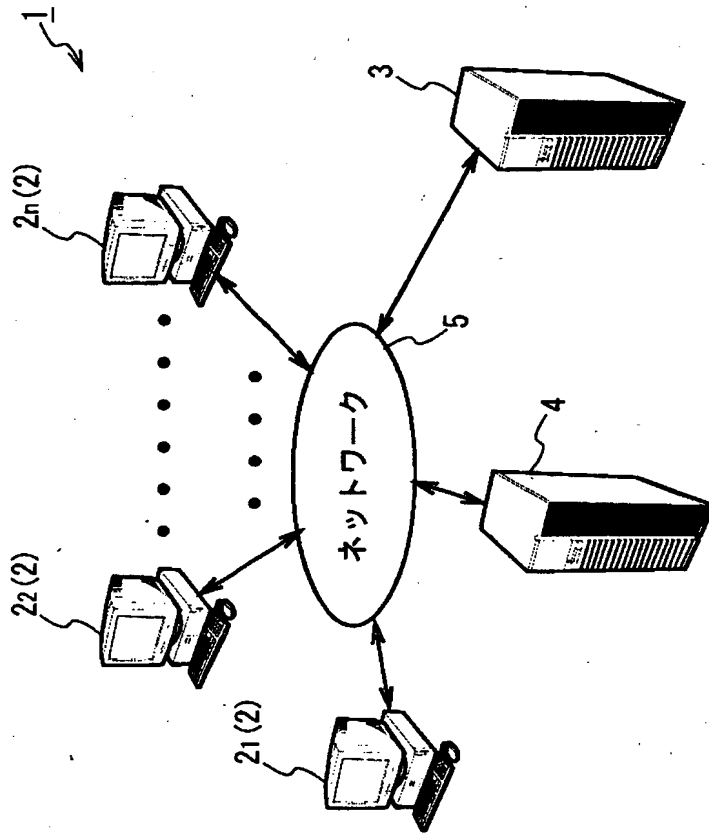


図1 第1の実施の形態によるコンテンツ配信システムの構成

【図2】

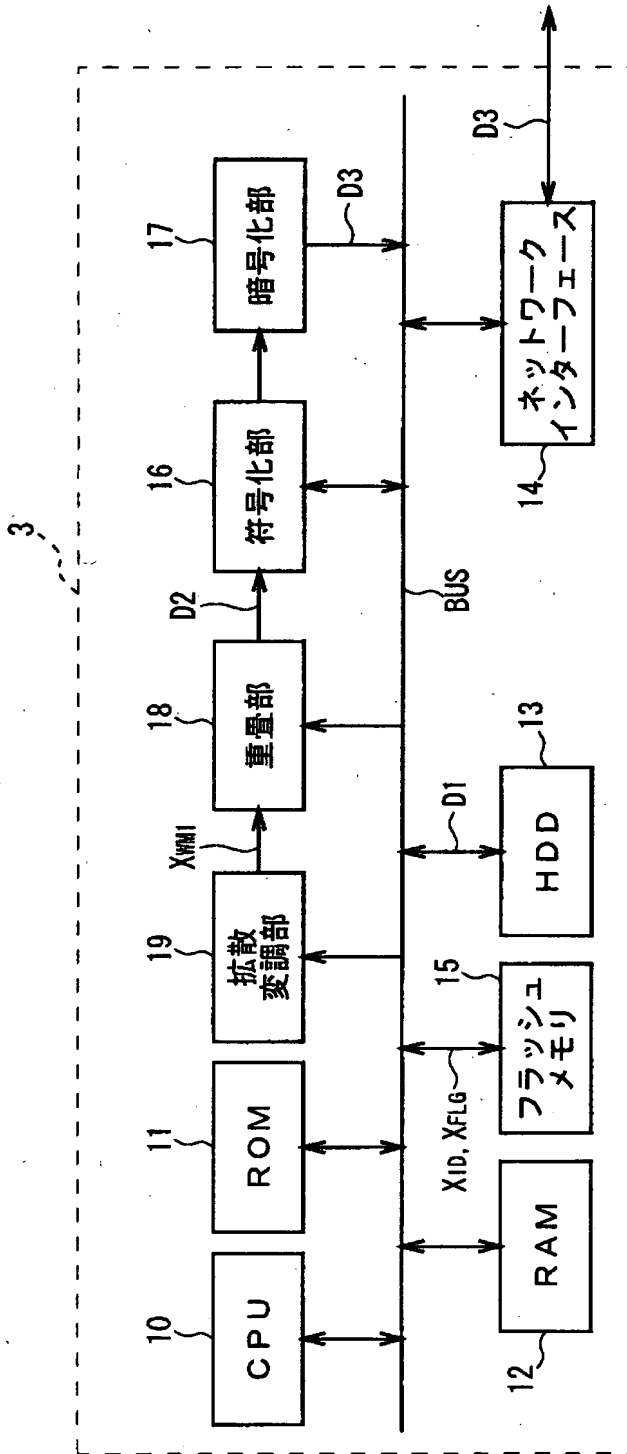


図2 第1の実施の形態による配信サーバの構成

【図3】

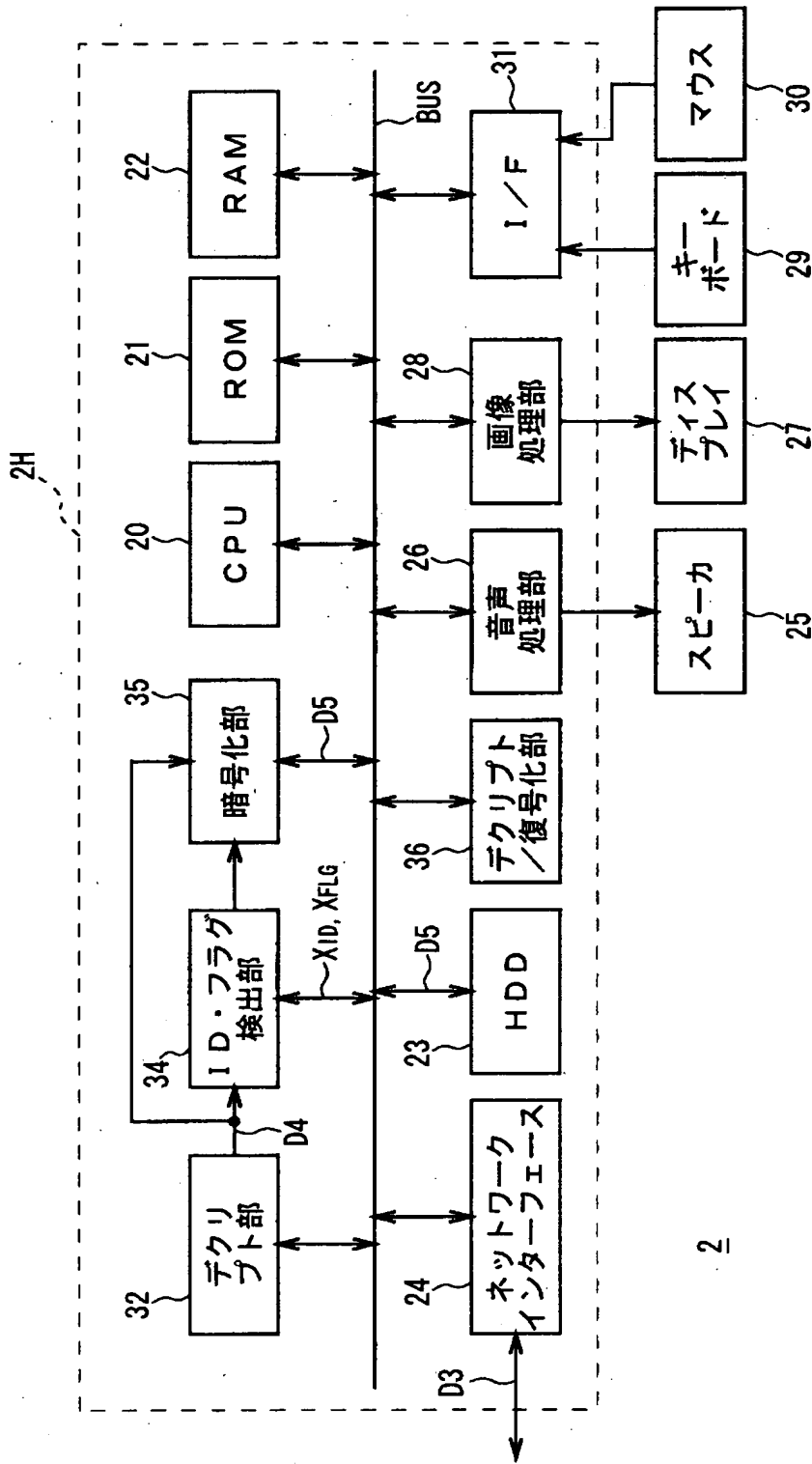


図3 第1の実施の形態による個人端末の構成

【図4】

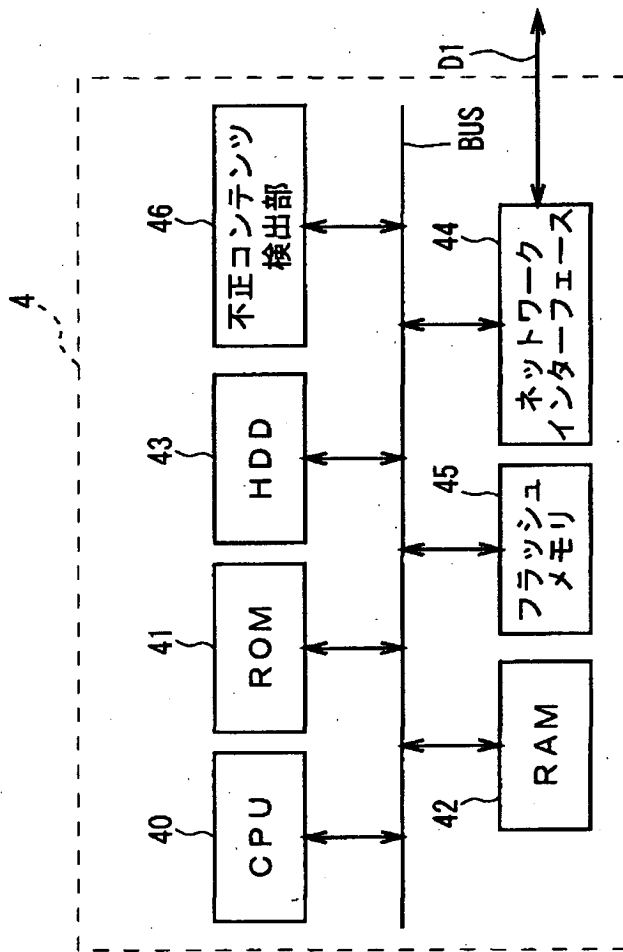


図4 第1の実施の形態による監視サーバの構成

【図 5】

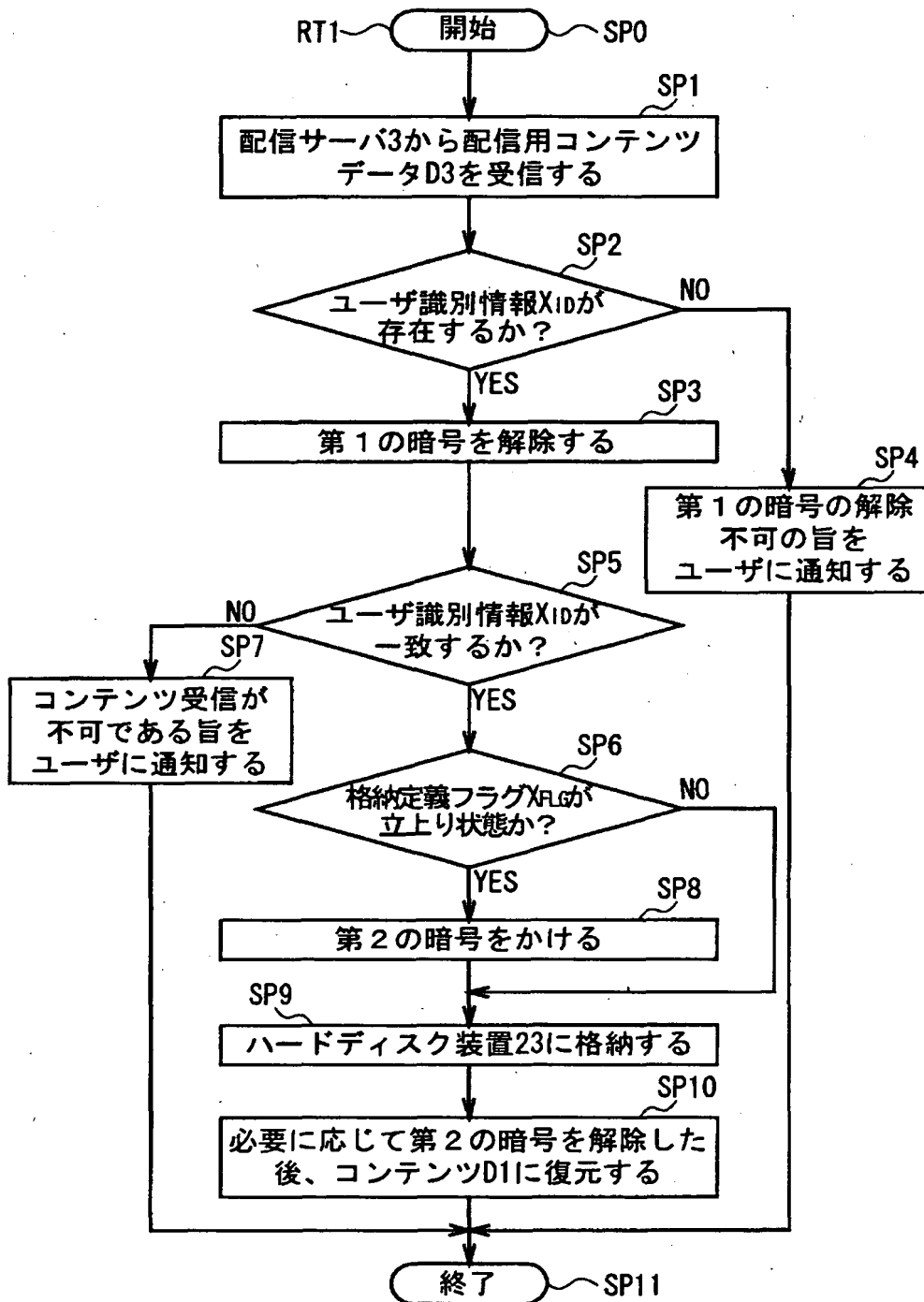


図 5 第 1 の実施の形態によるコンテンツ受信処理手順

【図6】

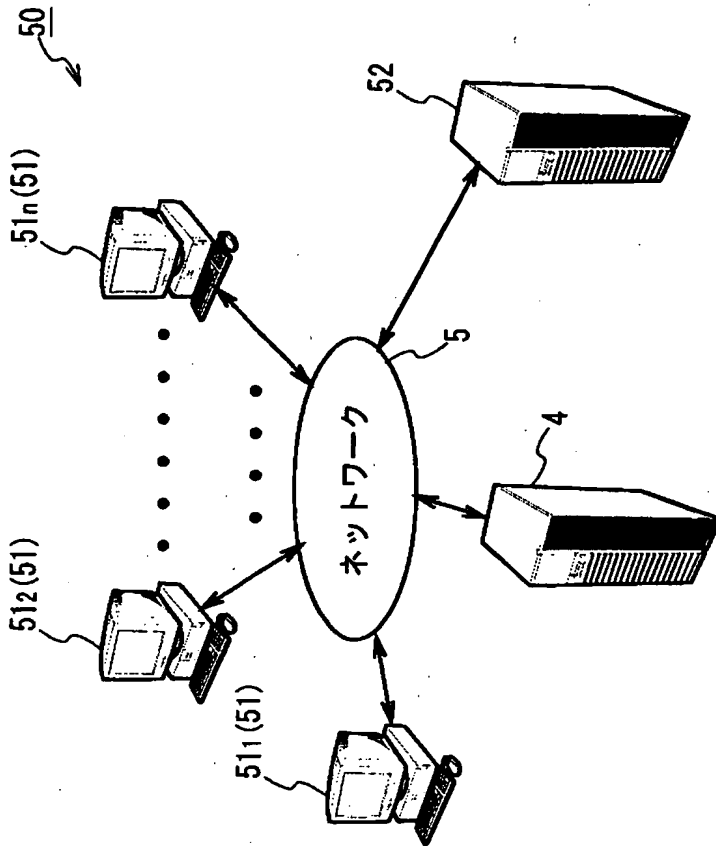


図6 第2の実施の形態によるコンテンツ配信システムの構成

52

【図 7】

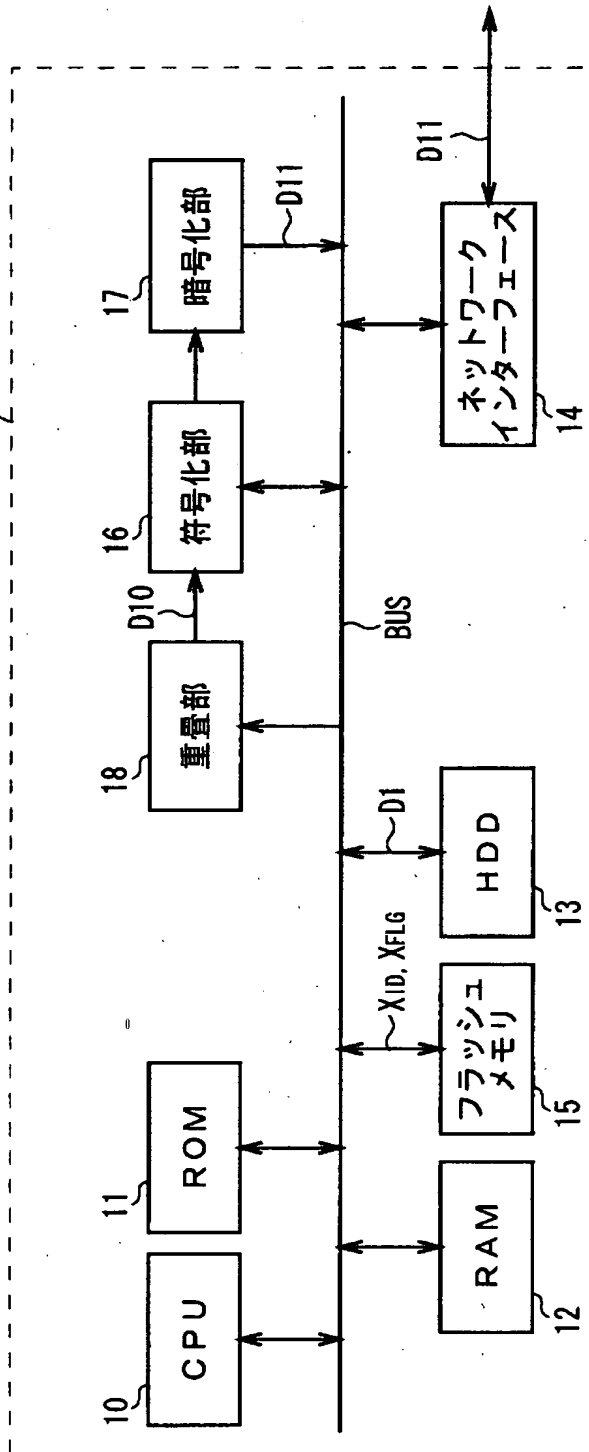


図 7 第 2 の実施の形態による配信サーバの構成

【图 8】

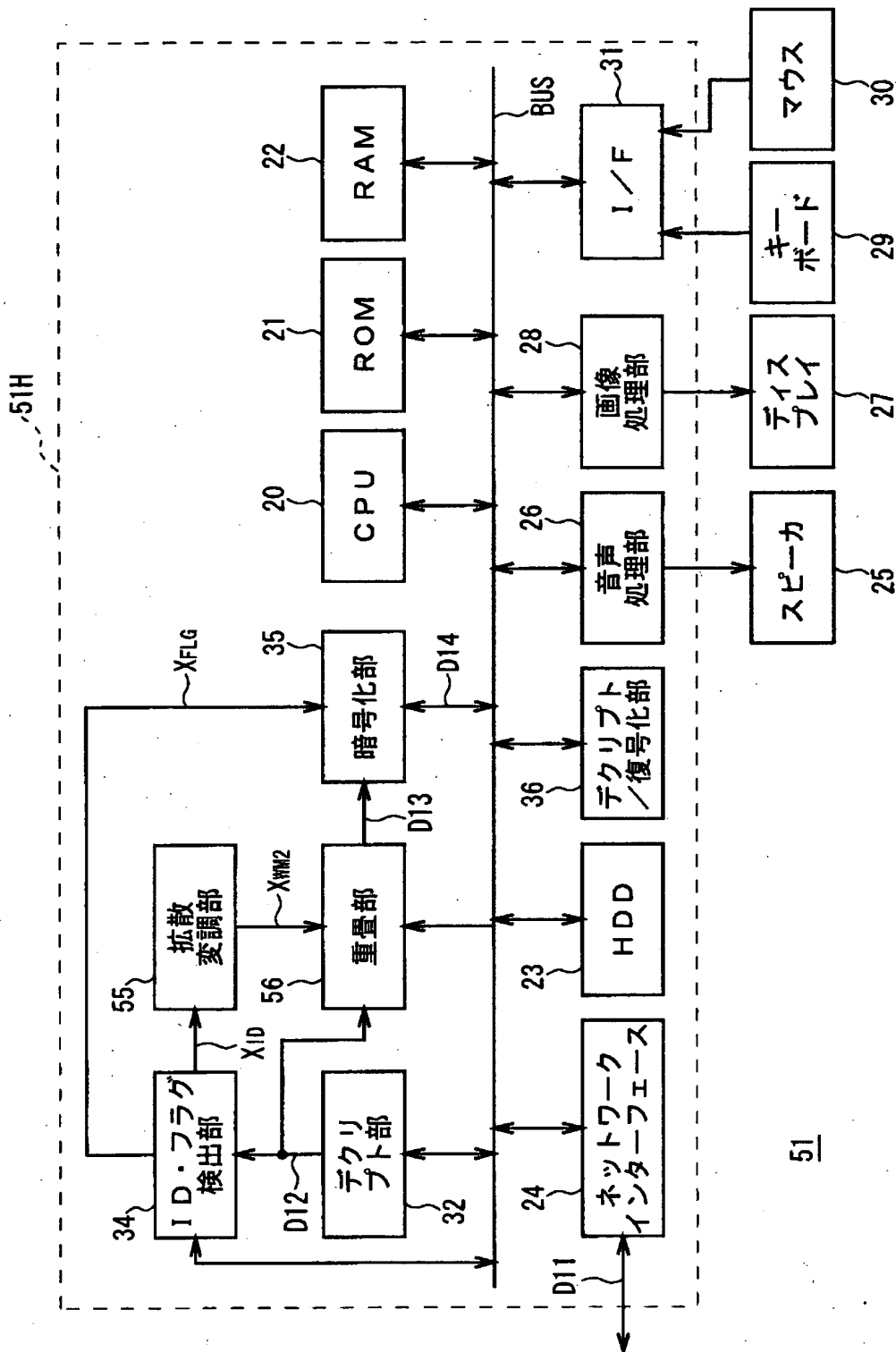


図8 第2の実施の形態による個人端末の構成

【図 9】

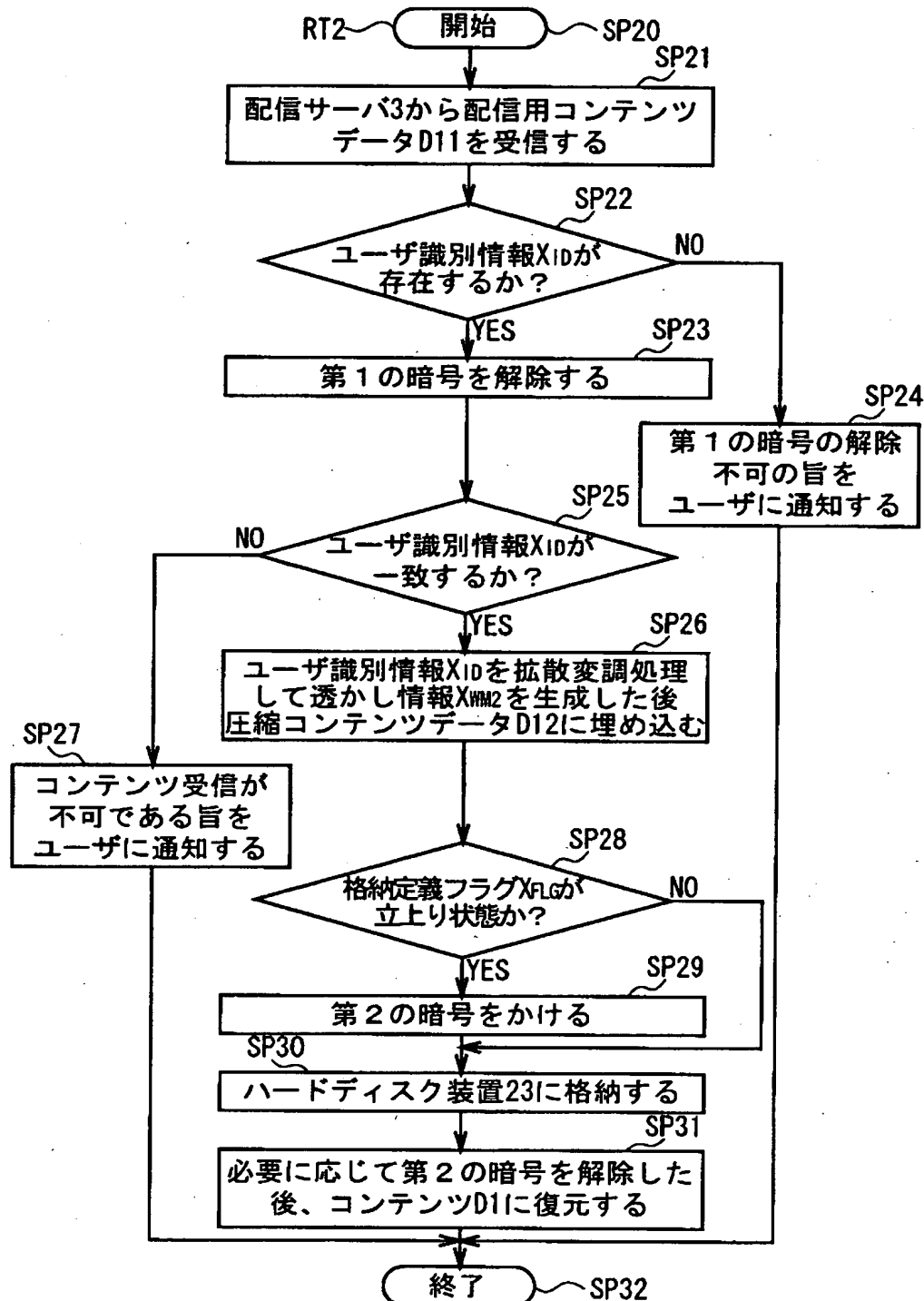


図 9 第 2 の実施の形態によるコンテンツ受信処理手順

【図 10】

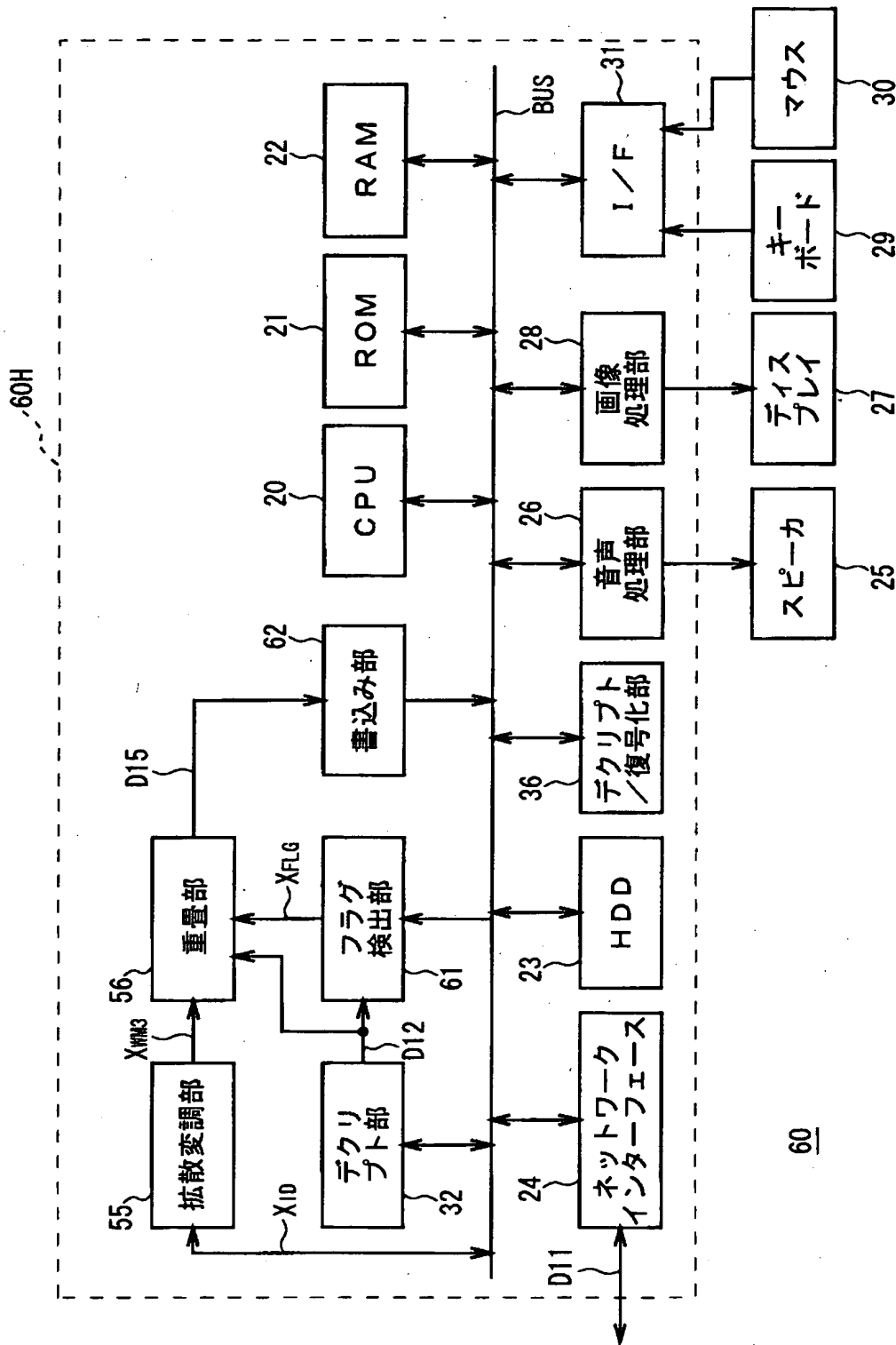


図10 第3の実施の形態による個人端末の構成

【図11】

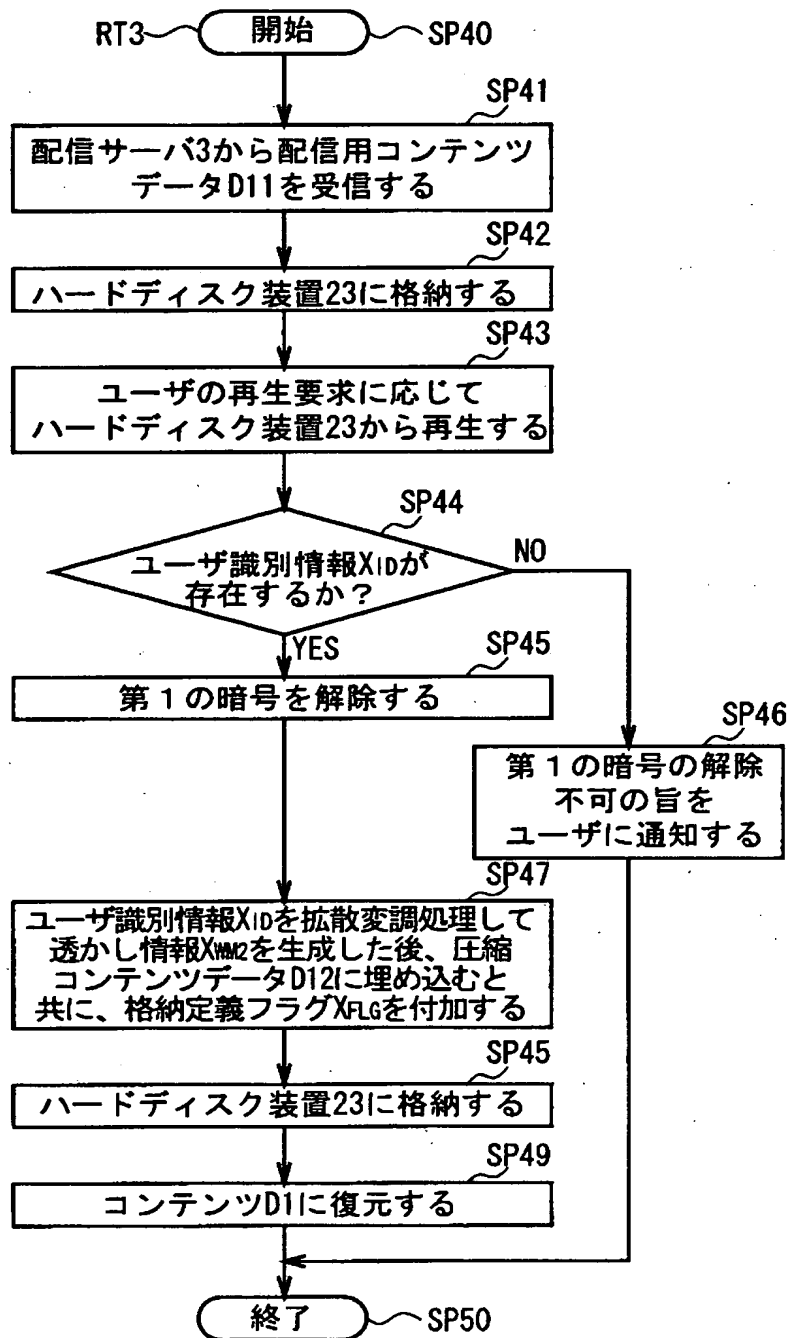


図11 第3の実施の形態によるコンテンツ受信処理手順

【図12】

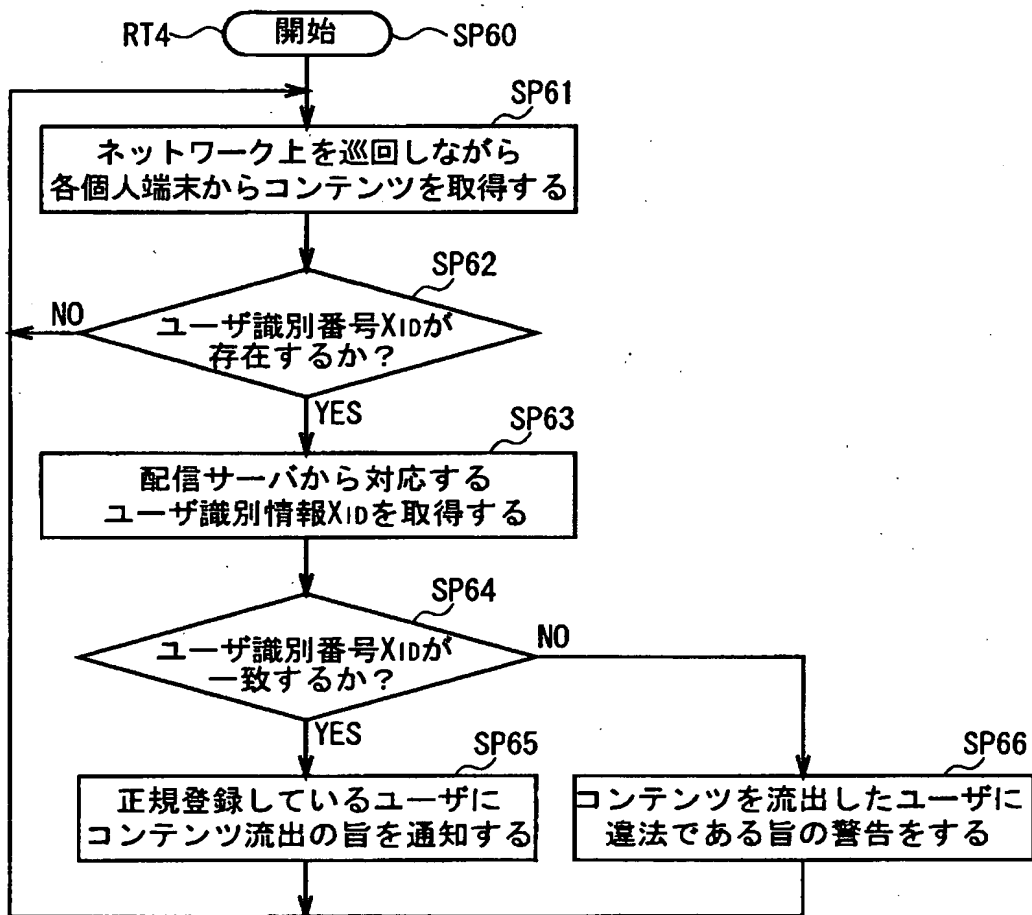


図12 異なるユーザに基づくコンテンツ監視処理手順

【図13】

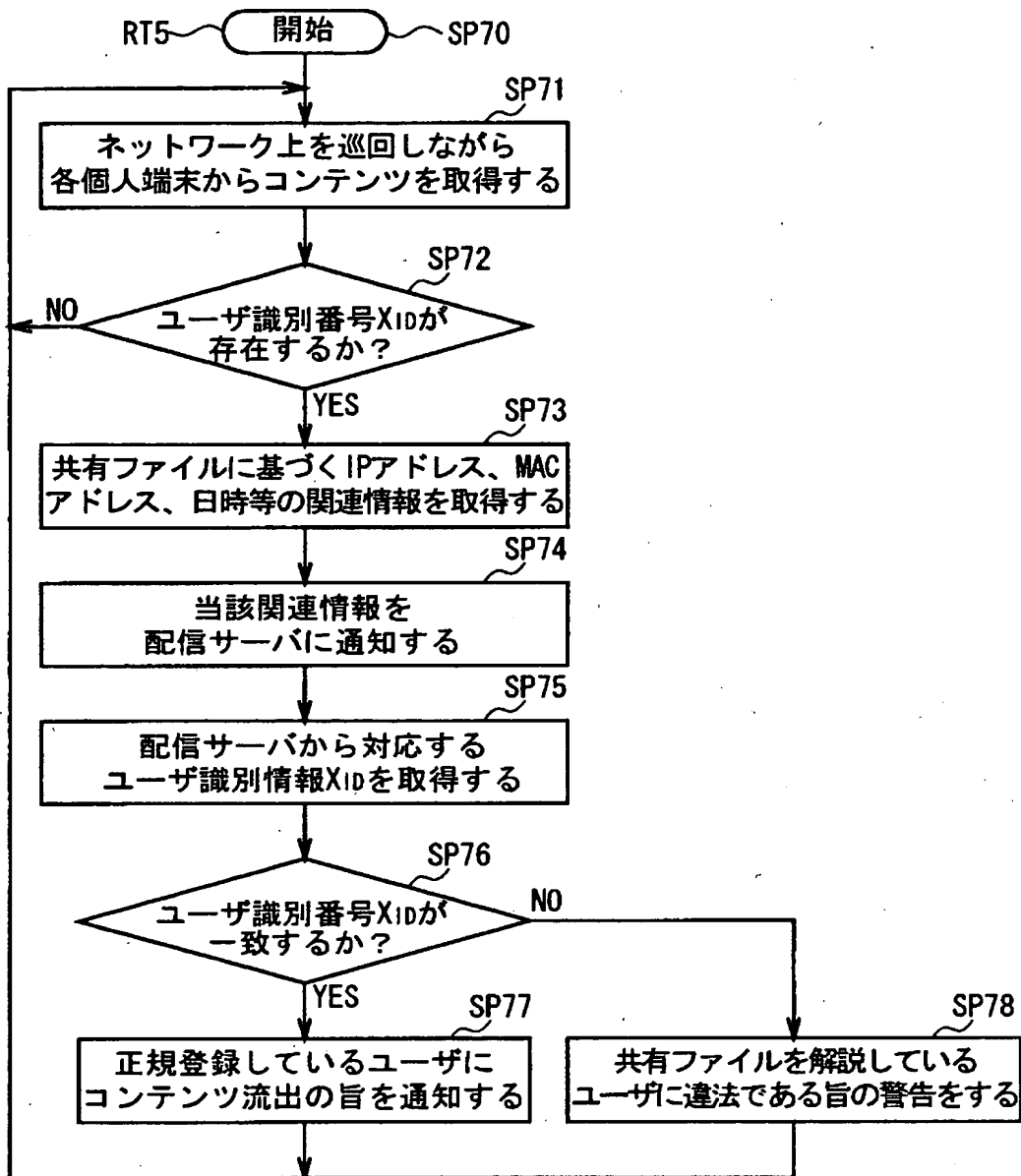


図13 ファイル共有に基づくコンテンツ監視処理手順

【書類名】 要約書

【要約】

【課題】

本発明は、正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム及びコンテンツ配信方法並びに端末装置を実現しようとするものである。

【解決手段】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随するようにして、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができるようにした。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社